Cybersecurity Pedagogy & Practice Journal

Volume 2, No. 1
April 2023
ISSN: 2832-1006

In this issue:

iscap
Information Systems
& Computing
Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

2023 ISCAP Board of Directors

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Editors

2023 Review Board

Educational Cyber Ranges: A Mixed-Method Study of Significant Learning Experiences using Cyber Ranges for Cybersecurity Education

Cheryl Beauchamp
cherbea@regent.edu
Department of Engineering and Computer Science
Regent University
Virginia Beach, VA

Holly Matuscovich
matushm@vt.edu
Department of Engineering Education
Virginia Tech
Blacksburg, VA

Abstract

Cybersecurity breaches and attacks have not only cost businesses and organizations millions of dollars but have also threatened national security and critical infrastructure. Examples include the Ransomware attack in May of 2021 on the largest fuel pipeline in the United States and the February 2021 remote access system breach of a Florida water treatment facility which raised sodium hydroxide to a lethal level. Improving cybersecurity requires a skilled workforce with relevant knowledge and skills. Academic cyber ranges offer virtualized environments that support cybersecurity educators' needs to provide students with a safe, separated, and engaging environment. More and more academic programs utilize cyber ranges due to the perceived benefit of integrating them into their cybersecurity-related programs. The purpose of this study was to understand the educators who were using the Virginia Cyber Range and how they were using them for cybersecurity education. More specifically, the study examined their usage for alignment with a learning taxonomy to verify the usage contributed to successful and significant student learning. Results suggested that high school cybersecurity educators were the primary users. These educators had less formal cybersecurity education and experience compared to cybersecurity educators in higher education. The data also showed that cybersecurity educators primarily used cyber ranges for teaching and learning as opposed to providing feedback and assessment to meet learning goals and objectives.

Keywords: cyber ranges, cybersecurity education, significant learning experiences, integrated course design

1. INTRODUCTION

Ranges are used to practice skills in a controlled environment. Golf driving ranges allow golfers to practice their golf swing before an actual game. A shooting range provides an opportunity to practice with firearms before a qualification test or competition. Similarly, cyber ranges provide a means for organizations to practice penetration testing and incident response in a simulated environment, providing realistic training. The military, government, and private industry use organizational cyber ranges such as the National Cyber Range, the DOD Cyber Security Range, and private cyber ranges such as Raytheon's, IBM's, and Metova's (Smith, 2017). Organizational cyber ranges train their personnel in an operational context and may include simulated scenarios with realistic networks that mirror the working environment (Brunner et al., 2019). These ranges utilize virtualization for efficiency and cost-effectiveness.

Nonetheless, virtualization software, installation, configuration, and support can be expensive (Brunner et al., 2019). Variations in cyber ranges exist to balance the needs of its users and resources. Specifically, differences in educational cyber ranges exist to meet the challenges of resources and support while also providing specific educational needs. Compared to organizational cyber ranges, academic facing cyber ranges in cybersecurity education are relatively new. The purpose of this study is to contribute to research on educational cyber ranges and cybersecurity education by describing who is using the Virginia Cyber Range (VaCR) for educational purposes and how they are using it.

For cybersecurity educators, a cyber range is a safe, virtual environment for activities that support cybersecurity-related hands-on learning (Darwish et al., 2020). Cybersecurity educators will most likely use cyber ranges in their classrooms to aid instructional content or assessment (NIST, 2018). They may also use cyber ranges outside of the classroom for professional development (PD) and enrichment activities (Beauchamp et al., 2020). A cyber range supports efforts to provide cybersecurity education with engaging hands-on exercises and labs to gain proficiency in a safe, virtual environment. Since the implementation of cyber ranges for educational purposes in academic settings is relatively recent, there is a need to explore and describe educational cyber ranges to develop theory and understand how these academic cyber ranges support cybersecurity educational efforts.

Accordingly, this research focuses on a single cyber range, the VaCR. Understanding how the VaCR supports teaching and learning may be valuable to others interested in investing in an educational cyber range. The results of studying the VaCR may transfer if future locations decide the approach is fitting for their needs (Tracy, 2010). The VaCR is an advantageous location to explore educational cyber ranges. Its purpose is specified for education, its cloud-based design increases its accessibility, and its multi-university collaboration provides an abundance of cybersecurity education resources.

The purpose of this study was to describe who are the educators using cyber ranges for cybersecurity education and how they are using them to create significant cybersecurity learning experiences from the educator's perspective. Using Fink's Significant Learning Experience (SLE) taxonomy (2013) as a theoretical lens, the study addresses the following research questions:

- Who are the educators using the VaCR for educational purposes?
- How is the VaCR used for cybersecurity education?

The analysis described how the VaCR is used through the perspective of its registered educators to provide an understanding of how cyber range resources are used by cybersecurity educators and who are the educators using them to support cybersecurity education.

2. CYBER RANGES: APPROACHES AND CURRENT USAGE LANDSCAPE

A single definition of cyber ranges does not exist as they have varying types, users, and purposes. Understanding cyber ranges in cybersecurity education requires understanding the types, the users, and the purposes. Additionally, the technological capabilities and approaches have changed through the years due to advancements in hardware and software capabilities, dating some of the prior research studies (Yamin et al., 2019). Previous studies tend to focus on a specific cyber range. They have not included an understanding of how cyber ranges are used for cybersecurity education from the perspective of cybersecurity educators.

A list of known cyber ranges and their capabilities is provided in Appendix A. This list and descriptions of cyber range providers, users, objectives, type of infrastructure, and deployment platforms was compiled from several prior studies (Babcock, 2019; Circadence, n.d.; Davis & Magrath, 2013; Georgia Technology Authority, n.d.; Hayman, 2019; National Cyber Warfare Foundation, 2019; Priyadarshini, 2019; Yamin et al., 2019). An Australian cyber range survey (Davis & Magrath, 2013) study compiled information to describe the approaches and functionality of existing cyber ranges to assist organizations when making informed decisions regarding cyber ranges. Their approach to cyber range classification was by who used the cyber range and the cyber range approach. The study is considered dated compared to current cyber range technology advancements and tools (Yamin et al., 2019). Yamin's study, conducted six years later, addressed the need for a more current study.

Yamin et al.'s literature review addressed the gap in research as previous studies were considered outdated or focused too specifically on one domain and did not provide a general understanding of cyber range systems (2019). The objectives of the review included identifying and classifying the cyber range functionality; evaluating cyber range approach and architecture model; classifying cyber range application as either training or testing; and identifying methods to assess different cyber ranges against a standard. The means for evaluation included the cyber range scenarios, functions, and tools.

These prior studies contribute to our understanding of the current cyber range landscape by providing definitions and categorizations. However, little is known about how educators use cyber ranges for cybersecurity education. As seen in Appendix A, there were nine academic providers of Cyber Ranges as of 2021. Only three academic cyber range providers identified education as their single objective. Although both the VaCR and the Arkansas Cyber Range limited their participants to academic participants, the VaCR provided Cloud access. A description of cyber range providers, users, objectives, type of infrastructure, and deployment platforms contribute to understanding the variances of cyber ranges prior to singling in on cyber ranges that are used for cybersecurity education. A description of each classification contributes to understanding who is involved with cyber ranges, their history, participants, stated objectives, and the characterization of their operations.

3. THEORETICAL LENS

Recognizing that educators with varying situational factors may apply different teaching activities and assessments to meet cybersecurity learning goals, this study used Fink's Integrated Course Design (ICD) framework (2005) to explore how Virginia educators used the VaCR for significant student learning experiences. Several prior studies have applied Fink's Significant Learning Experience taxonomy and ICD framework principles to courses in several disciplines. These include a health policy course (Krueger et al., 2011), a psychology program course (Fallahi, 2008), a nursing program course (Marrocco, 2014), and a sustainability engineering course (Apul & Philpott, 2011). These studies used the principles to redesign existing courses and evaluate the changes against Fink's Significant Learning Experiences taxonomy. This study differs in that it investigates existing elements in current educational practices versus studying their intentional implementation as in these prior works.

According to Fink's model, educators' situational factors influence the teaching and learning activities, the feedback, and the assessments integrated within their courses to meet the learning goals (Fink, 2005). Fink's work claims that this ICD contributes to significant learning experiences for students (Streveler et al., 2012; Fink, 2013). Significant learning consists of six dimensions of learning categorized as Foundational Knowledge, Application, Integration, Human Dimension, Caring, and Learning How to Learn (Fink, 2013). These categories interact to contribute to significant learning.

These six categories of significant learning formulate the learning goals in the ICD framework. The components of ICD, including the learning goals, situational factors, teaching and learning activities, and feedback and assessment, are interconnected. The learning goals provide the means for formulating the appropriate feedback and assessment procedures. These, in turn, provide the necessary understanding to select effective teaching and learning activities. Foundational to these components are the situational factors that may impact them.

Situational factors may affect decisions regarding the learning goals, the feedback and assessment, and the teaching and learning activities. These factors include the context of the teaching and learning situation, the nature of the subject, the characteristics of the learner and teacher, and any particular pedagogical challenges. Pedagogical challenges are situations that may present challenges to the students or the educator and the opportunity for significant learning (Fink, 2013).

Using the ICD components to explore how educators used cyber ranges, a special pedagogical challenge (Fink, 2013), provided an encompassing understanding of how educators use cyber ranges for significant cybersecurity learning. The findings described how they used the cyber range to support teaching and learning activities, provide feedback to students, and assess students' learning.

4. METHODS

This study drew upon both quantitative and qualitative data to understand the VaCR registered educators and how they used the VaCR for cybersecurity education. This study contributes to a larger case study to understand cyber ranges in cybersecurity education through the educator and student perspectives. The VaCR was the unit of analysis for this study. The data sources were educator responses to a questionnaire and data sources from the VaCR, such as their website and traffic data. This study was conducted in accordance with the university human subject's research requirements and necessary ethical considerations to protect the educator participants.

Case Site Description
The VaCR was created in 2016 with the mission to enhance cybersecurity education and increase the number of students entering the cybersecurity workforce (Virginia Cyber Range, n.d.) Since the VaCR was designed and developed specifically for education, the data associated with its users, usage, and resources contribute to educational purposes. This academic focus enables findings from this study to correlate educational efforts related to the cyber range compared to a cyber range that may have mixed users, usage, and resources.

The VaCR is cloud-based, accessible via a web portal. Users are not required to purchase supporting software, configure hardware, or pay expensive access fees. Its resources are openly available to Virginia public educational institutions. The registered users are students and faculty in over 200 high schools, community colleges, and universities. According to the cyber range registration data provided by the Communications and Development Manager for the VaCR, over half of the VaCR registered educators in 2020 were high school educators (Lawrence-Kuether, 2020). Accessibility is supported by over 50,000 deployed virtual machines (Virginia Cyber Range, n.d.). The VaCR approach of hosting their cyber range in the cloud provides rapid scalability and low-cost investment with fees associated with usage. The cyber range is not location-dependent and is accessible globally via a user login through their web portal.

As of 2021, the VaCR is advised by members from public higher education institutions in Virginia that have been nationally designated as Centers of Academic Excellence in Cybersecurity by the National Security Agency and the Department of Homeland Security. There are 17 colleges and universities with this designation on the advisory committee, and this status continues to expand as more public Virginia colleges become designated. Through this multi-college and university partnership, the VaCR provides an extensive courseware repository of courses, labs, workshops, lessons, and environments (Raymond, n.d.).

Data Collection
The data sources were responses to an anchored open-ended (AOE) questionnaire, the VaCR website, and traffic data provided by the administrators of the VaCR to gather resource usage. The primary data source, the AOE questionnaire, included in Appendix B, was sent to the registered educators of the VaCR to obtain a sample of cybersecurity educators. there were 85 educators who participated in the study. Since the study did not require personal educator identification, identifiable information such as the participants name was not included to protect the participant's identity. Communication with the VaCR administrators provided traffic data reports.

Sampling Plan
This study used a purposive non-probability sampling approach to study who uses the VaCR and how they use it (Trochim, 2006). The reason for purposefully selecting the Virginia/US Cyber range was its ability to meet specific criteria to include its focus on cybersecurity education versus the other cyber ranges included in Appendix A. The Virginia Cyber Range is only accessible to educators via required registration. The questionnaire was sent to all the registered members to provide a means to obtain a diverse, heterogeneous sampling (Trochim, 2006). Due to the small population of VaCR registered educators, this study used follow-up emails and a gift card drawing incentive to encourage higher response rates. Although 85 educators contributed different levels of questionnaire responses, 70 of them reported using the VaCR during the 2020 – 2021 academic year.

AOE Questionnaire and Traffic Data
An AOE questionnaire uses the responses to closed-ended questions as foundations (or anchors) for accompanying responses to open-ended questions. Lee & Lutz (2016) found that AOE questions provided the ability to sort a large number of responses more quickly than open-ended questions and more accurately than closed-ended questions. The instrument for this study used closed-ended questions to capture information regarding who the VaCR registered educators were, what they taught, and which VaCR resources they used. The instrument also included open-ended questions to further record information to corroborate and explain participants' answer choices for the closed-ended questions. For example, in addition to recording which VaCR resources they used for assessment, respondents were asked to provide examples of

how they used the cyber range to support their assessment efforts.

A prior conference panel discussion with four Virginia high school cybersecurity educators (Beauchamp et al., 2020) provided initial insight regarding how they used the VaCR. This insight contributed to the initial design of the instrument questions. Additionally, two VaCR educators reviewed the instrument and provided their feedback for content validity, clarity of the questions, and overall ease of completing the instrument.
The VaCR traffic data was used to corroborate and triangulate the questionnaire responses regarding the VaCR resources educators utilized.

Analysis

The open-ended responses to the AOE questionnaire were analyzed qualitatively using in vivo and descriptive coding (Miles et al., 2020; Saldana, 2016). The coding used the ICD components of teaching and learning, assessment and feedback, and significant learning goals as the lens to explore how educators use cyber ranges. Appendix C includes partial tables for each of the coding steps.

A fellow qualitative researcher cross-checked codes using the developed codebook (Creswell & Creswell, 2018). Their review and coding addressed inter-rater reliability (Creswell & Poth, 2018).

Analysis of the closed-ended questions for educator information included who used the VaCR and how they used it. These traffic data reports were analyzed to determine which resources were utilized, the time duration of use, and the frequency of use. The VaCR website described the available educational resources. The traffic report data and resource description were used to triangulate questionnaire data.

5. FINDINGS

In addressing the first research question, although the stated mission of the Virginia Cyber Range is to enhance cybersecurity education for students at the high school and post-secondary levels (Virginia Cyber Range, n.d.), results showed that high school educators are the primary users of the VaCR for cybersecurity education, and they are predominantly male, with 67.4% of the participants identifying as male. This is a higher percentage compared to the national percentage of male computer science high school educators. Although cybersecurity educators are primarily Career and Technology Educators, some educators may also be certified as Computer Science teachers. According to an estimate that was verified against the Bureau of Labor and Statistics, 53.6% of high school computer science teachers identified as male (Zippia Careers, 2021). Additionally, results showed that high school educators had less formal technical education, experience, and certifications than those in higher education, but they utilized online workshops more than their counterparts. Those who taught cybersecurity for the first time were all high school educators. For purposes of this study, these first-time cybersecurity educators are referred to as novices.

Educators who use VaCR for Cybersecurity Education

VaCR educators are primarily high school educators. As seen in Figure 1, high school educators make up more than half (52%) of the educators who use the VaCR. The other half were higher education educators at community colleges (17%), universities and colleges (28%), and educators who did not identify their level of teaching (3%).

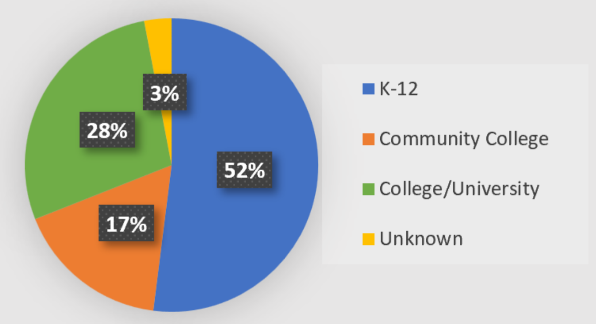


Figure 1: VaCR Registered Virginia Educators

The educators who responded to the study reflected a similar composition of instruction-level as the overall population of VaCR registered educators, as seen in Figure 2.

VaCR educators teach technical, business, and STEM courses. Virginia educators who used the VaCR in 2020-2021 taught technology courses: Cybersecurity Fundamentals, Introduction to Programming, Computer Networks, Digital Forensics. The high school educators also taught business, science, and math courses. A list of courses taught in 2020 - 2021 is provided in Appendix D.

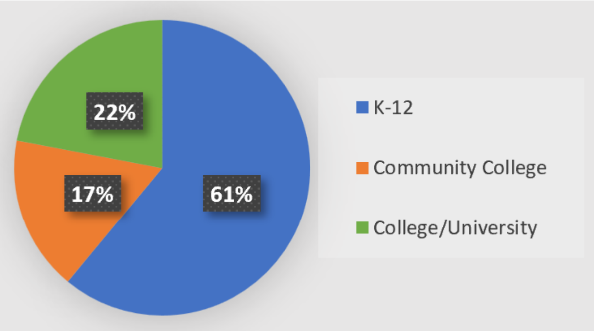


Figure 2: Breakdown of Study Participants

46 of the 70 participants who used the VaCR provided gender information. These educators primarily identified male (67%) versus female (33%). Figure 3 reflects the gender representation at the high school, community college, and university/college levels from those who reported gender identification information. The question format followed engineering education recommendations for more inclusive approaches to collecting demographic data such as providing a gender continuum (Fernandez et al., 2016). Utilizing their recommended approach, the question stem uses gender, and the choices are actually for participant sex, so we report the results as the question was asked.

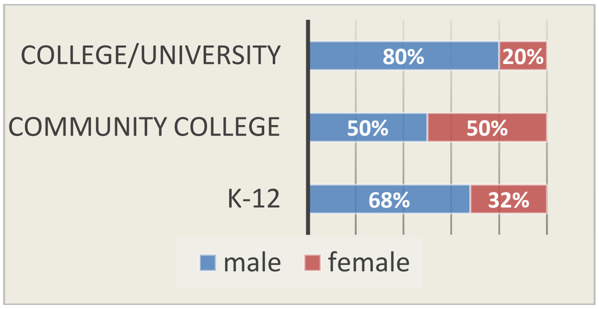


Figure 3: Gender of VaCR Educators

Educators were primarily White (59%), but others also identified as Black or African American (9%), Hispanic, Latino, or Spanish origin (4%), or Asian or Asian American (2%) as depicted in Figure 4.

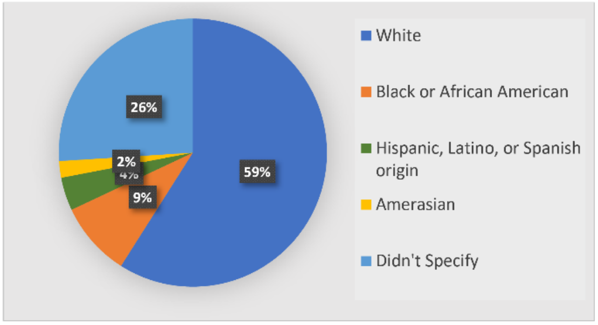


Figure 4: Racial Groups of VaCR Educators

High school educators had less professional technical experience, industry certifications, and formal academic courses in cybersecurity than higher education educators but more involvement in Communities of Practice (CoPs), Informal Learning Communities (ILCs), and other sources for preparation; primarily the GenCyber program. They and community college educators also utilized online workshops. Six high school educators identified as novices; they taught a cybersecurity course for the first time in 2020 - 2021. There were no novices at the community college or the university/college level. The reported prior education, preparation, or experience are shown in Figure 5.

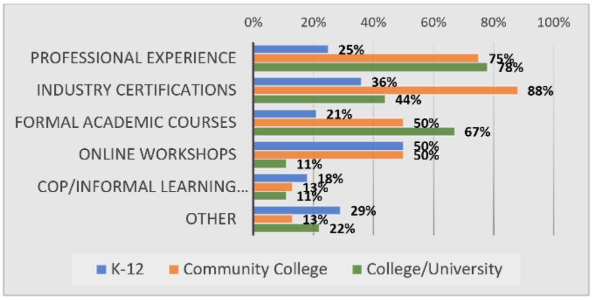


Figure 5: Prior Preparation and Experience of VaCR Educators

68% of high school cybersecurity educators stated they held a Virginia education teaching license. Currently, cybersecurity licensure is unavailable in Virginia. Many educators reported having business and technology licensure as cybersecurity-related courses are offered in the Career and Technical Education programs. Other educators reported licensure in Computer Science, Physics and Math, or Business & Marketing. One educator listed their licensure in Business, English, Physical Education, and Social Sciences.

VaCR usage for Cybersecurity Education

The results regarding the second research question show that educators primarily use the VaCR for teaching and learning activities. Although the VaCR was not currently or widely used for providing feedback and assessment, educators shared that they would like to use the VaCR more when they have time and understanding of how to utilize it for effective feedback and assessment. The results also demonstrated that educators who used the VaCR provided significant learning experiences as their usage addressed the six constructs of the significant learning goals.

Results showed that educators primarily use the VaCR for its hands-on labs and its CTF tool (See Figure 6). Some educators created their own labs, but others reported using Brigante, Metasploit, Kali Linux and Windows, Linux Intro, labs related to password cracking and auditing, Ubuntu, and labs that supported tools such as Nmap, JTR, Wireshark, Snort, Mcrypt, and DVWA for scanning. Other resources included instructional information, curriculum development, and operating system virtual machines.

A lack of awareness of the other resources may be a reason for low reported usage as one high school novice educator shared, "I was unaware of any videos, weekly workshop series, etc. I went into teaching Cybersecurity with no preparation, few materials, and was advised by the previous teacher to join the cyber range."

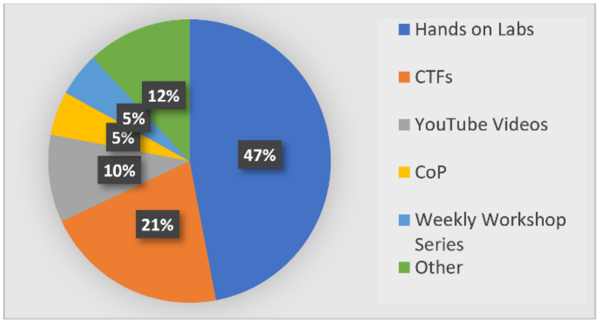


Figure 6: VaCR Resource Usage

Teaching and Learning Activities

Educators at all instructional levels reported similar usage of the VaCR for teaching and learning. The accessible and ready-to-use environments, such as the Kali Linux, Windows Virtual Machine, Ubuntu, and Brigante, provided online accessibility for students to work with cybersecurity tools safely.

The accessible environment also provided educators the means for their students to use cybersecurity tools and operating system commands in a safe and protected environment. The ability to apply and practice using tools, such as Wireshark and Linux commands, they learned about in class was another way educators used the VaCR to reinforce their teaching and learning activities. Although some educators created their own labs in the VaCR environment, others reported using the existing labs and lessons which mapped to their learning objectives.

Educators also used the CloudCTF tool for teaching and learning. Some utilized it as homework assignments, others as an assessment tool, while still others as a demonstrative tool. Appendix E provides excerpts from educators regarding their usage of the VaCR for teaching and learning activities.

Feedback and Assessments

Educators at all instructional levels shared using the VaCR for formative assessment, summative assessment, and feedback. However, they used it primarily for summative assessment purposes. Educators used the labs, working environments, and CTFs to assess student learning. Some shared that they did not use the VaCR for feedback, that although they did not currently use the VaCR for assessment or feedback, they plan to do so in the future. As stated by one experienced college-level educator, "I do not currently use it in my assessments right now but will eventually use it in the future." Appendix F provides excerpts from educators regarding their usage of the VaCR for feedback and assessments.

Learning Goals

All six dimensions of Fink's (2013) Significant Learning Goals were evident from educators using the VaCR for cybersecurity education. Although educators did not expressly state their teaching efforts aligned with the goals, their descriptions of how they used the VaCR demonstrated their teaching efforts supported their students' abilities to meet these learning goals.

Foundational Knowledge: Students remember and build an understanding of cybersecurity information by using the labs, environment, and CTFs, both in and out of class. This usage provides means for students to build their foundational cybersecurity knowledge.

Application: Students learn how to apply new learning via the VaCR hands-on activities and environments. This hands-on application requires critical, creative, and practical thinking skills and time management and content knowledge to further their skills. Using the labs, environment, and CTFs, students learn new actions: new skills and ways of thinking. For example, this educator shared that he used the VaCR "for my labs and homework to give the students a better source for practicing using the tools and other information involving the fundamentals and frameworks."

Integration: Working with VaCR resources, students connected various subjects such as programming, networks, and cybersecurity fundamentals as well as group or team skills and project management. Through this integration, students connect various subject areas and learning experiences, including team/group work activities. One educator stated he used the "cyber range environment for application of network reconnaissance, footprinting, and enumeration principles" and for "application of firewall, IDS configuration principles and public key cryptography concepts.”

Human Dimension: students build new connections with themselves and others when they apply their course knowledge in labs that provide hands-on practice and opportunities to work with others. For example, one educator shared that although his students had individual assignments, he encouraged them to work with each other to learn different strategies for achieving the learning objectives of the assignment, “students are permitted to network with their class peers on the assignments. I find that the students learn by discussing options & strategies for achieving objectives with their peers.”

Caring: Educators shared students experienced positive engagement when using the VaCR. Educators also shared that this positive engagement reinforced their students' interest in cybersecurity using the cyber range. Students develop interest or value for cybersecurity with the positive and active learning engagement when using the VaCR. According to Fink, “the development of new interests, feeling, and values” contribute towards the caring component of significant learning (2013, p.83). An educator shared that he uses the VaCR as a reward, “students enjoy the gamification aspect of the CTFs,” while another educator shared that he finds using the VaCR rewarding due to his students’ positive engagement using the VaCR, “Their excitement of successfully completing the [Denial of Service] lab was contagious.”

Learning to Learn: The labs, environment, and CTFs also provide students an opportunity to become better cybersecurity students and self-directed learners. One educator stated, “My students like the [Virginia Cyber Range] range as a self-directed tool that gives them a break from my lectures.”

Limitations

As with all studies, this research has limitations. They do not invalidate the findings but should be considered. The population of VaCR registered educators was purposefully selected to study the VaCR; therefore, the transferability of findings from the VaCR to another cyber range may be limited. However, the "fittingness" of the findings to the reader's own experience and situations (Krathwohl, 2009, p. 350) was supported through rich and detailed descriptions. Additionally, VaCR educators who participated did so voluntarily. Thus, self-selection bias might exist, and the sample may skew towards educators who had strong opinions towards using cyber ranges. Therefore, this study may not represent all views and does not claim to do so.

Another limitation is the small sample size due to the small population of VaCR registered educators. These VaCR users are mostly high school level cybersecurity educators, while other cyber ranges may have more users at the post-secondary level. The low response rate was an additional limitation which may have been due to varying factors, including the timing of the questionnaire in the academic school year, or due to the impact of COVID-19. Again, this study does not make claims of generalizability but instead contributes as an exploratory study of educators who use the VaCR and how they use the VaCR for cybersecurity education.

6. DISCUSSION & IMPLICATIONS

Discussion

Findings from this study support the usage of cyber ranges for cybersecurity education to provide Significant Learning Experiences. Results show that VaCR supported the three components of the ICD framework, as seen in Figure 7. Educators shared that the virtual environment is a safe and accessible environment for users to apply concepts presented in class to develop application skills and reinforce student understanding of cybersecurity-related concepts. The ready-to-use and customizable labs, lessons, and CTFs provided hands-on practice that contributed to teaching and learning activities. The VaCR also provided a means for feedback and assessment, though some educators did not report widely utilizing this capability yet. Nonetheless, educator usage of the VaCR also reflected the ability to address all six dimensions of Fink’s Learning Goals for providing Significant Learning Experiences (2013).

However, educators shared a lack of awareness of the different VaCR resources to assist their full usage of the VaCR. Some educators were assigned to teach cybersecurity and were not prepared to do so. Advised to utilize the VaCR, they were left to learn how to use it independently.

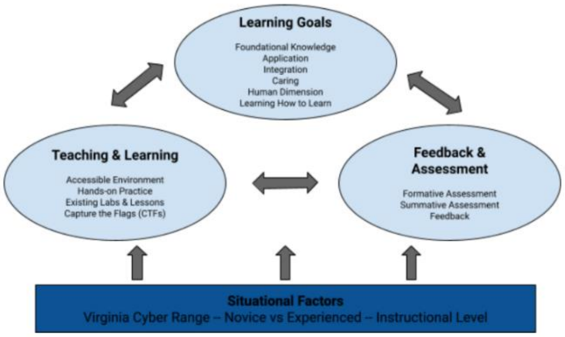


Figure 7: Educators' Usage of VacR Alignment with Fink's Significant Learning Experiences and ICD

Over half of the educators using the VaCR were high school educators with limited prior preparation or experience in cybersecurity education. These high school educators teach STEM, business, and technical courses as their primary teaching disciplines, as reflected in their state teaching licenses. Although the VaCR resources include workshops and videos to assist educators throughout the year, they were not widely used, perhaps because educators were unaware of these resources or did not have time for PD during the school year. High school educators shared they are more likely to engage in PD opportunities offered during the summer. They reported utilizing online and summer workshops for further PD.

Implications

The primary implication from this study is that cyber ranges in cybersecurity education support efforts to provide significant learning experiences. However, the integration will have limited success if the educators are not provided the necessary training and resources to support their efforts to utilize these ranges. Cybersecurity and cyber range stakeholders need to create a curriculum, instructor guides (w/solutions), and content that maps to cybersecurity learning objectives. PD programs should include awareness of these resources and how to use them. Cybersecurity and cyber range stakeholders need to create and facilitate PD offerings for novice educators, and they need to collaborate on associated research efforts.

Additionally, secondary education administrators who provide cybersecurity-related courses in their schools can support cyber range integration in those courses knowing the integration supports significant learning. However, this integration requires supporting cybersecurity educators with time and resources to pursue cybersecurity and cyber range-related PD. Educators can integrate cyber ranges in their cybersecurity-related courses with administrative support and attend cyber range and cybersecurity education PD opportunities.

Although the VaCR currently provides additional educator support resources to include Workshops Series and YouTube videos, findings from this study show educators did not report utilizing these resources. Further research is necessary to understand why VaCR educators did not widely use these resources. This understanding supports cyber range developers and stakeholders' ability to provide and update resources from which their educator users would benefit.

Continued research collaboration of all the stakeholders will also provide a further understanding of cyber ranges in cybersecurity education. Future studies include comparing usage by instructional levels and by experience level. Follow-up studies regarding differences in educator cyber range usage based upon gender, size of class enrollment, novice vs. experienced educator, core subject area, and prior preparation can use the questionnaire instrument from this study. These other areas are identified as situational factors for designing significant learning experiences – specific context of the teaching and learning situation and the characteristics of the educator (Fink, 2013). Future studies may include looking at some of these other situational factors and how they are related to using cyber ranges.

7. REFERENCES

Apul, D. S. & Philpott, S. M. (2011). Use of outdoor living spaces and fink's taxonomy of significant learning in sustainability engineering education. Journal of Professional Issues in Engineering Education and Practices, 137(2), 69-77. doi:10.1061/(ASCE)EI.1943-5541.0000051

Babcock, S. (2019) Economic leaders paid a visit to Maryland cyber centers. Technically Media. https://technical.ly/baltimore/2019/02/21/georgia-economic-leaders-paid-a-visit-to-maryland-cyber-centers/

Beauchamp, C., Frey, E., Marden, J., Rice, K., & Riggleman, K. (2020). At the center of cybersecurity education: The Virginia cyber range. Virginia Cybersecurity Education Conference, July 27-28, 2020. (Virtual).

Brunner, R., Oh, S. K., Ramirez, J., Houck, P., Stickney, N., & Blaine, R. (2019). Design for an educational cyber range. Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security. Nashville, TN. (April 1-3, 2019).

Circadence. (n.d.) Helping cyber professionals prepare and protect. Circadence. https://www.circadence.com/company/about/

Creswell, J. W. & Poth, C. N. (2018). Qualitative inquiry & research design: Choosing among five approaches (4th ed.). Thousand Oaks, CA: Sage.

Darwish, O., Stone, C. M., Karajeh, O., & Alsinglawi, B. (2020). Survey of educational cyber ranges. In: Barolli L., Amato F., Moscato F., Enokido T., Takizawa M. (eds) Web, Artificial Intelligence and Network Applications. WAINA 2020. Advances in Intelligent Systems and Computing, 1150. Springer, Cham. https://doi.org/10.1007/978-3-030-44038-1_96

Davis, J., Magrath, S. (2013). A survey of cyber ranges and testbeds. Defense Science and Technology Organization Edinburgh (Australia) Cyber and Electronic Warfare Division. Dicke A-L, Safavian N. & Eccles, J.S. (2019) Traditional Gender role beliefs and career attainment in STEM: A gendered story? Frontiers in Psychology,10(1053). doi: 10.3389/fpsyg.2019.01053

Fallahi, C. R. (2008). Redesign of a lifespan development course using fink's taxonomy. Teaching of Psychology, 35(3), 169-175. doi: 10.1080/00986280802289906.

Fernandez, T., Godwin, A., Doyle, J., Verdin, D., Boone, H., Kirn, A., Benson, L., & Potvin, G. (2016). More comprehensive and inclusive approaches to demographic data collection. School of Engineering Education Graduate Student Series. http://docs.lib.purdue.edu/enegs/60

Fink, L. D. (2003). What is significant learning. University of Oklahoma Significant Learning Website, Program for Instructional Innovation at the University of Oklahoma.

Fink, L. D. (2005). Integrated course design. The IDEA Center. https://www.ideaedu.org/Portals/0/Uploads/Documents/IDEA%20Papers/IDEA%20Papers/Idea_Paper_42.pdf

Fink, L. D. (2013). Creating significant learning experiences: An integrated approach to designing college courses. San Francisco, CA: Jossy-Bass.

Georgia Technology Authority. (n.d.) Georgia Cyber Center. Georgia Technology Authority. https://gta.georgia.gov/georgia-cyber-center

Hayman, S. (2019). Cyber range: New platform and degree readies students for cyber defense. University of Central Arkansas Magazine. https://uca.edu/magazine/cyber-range/

Krathwohl, D. R. (2009). Methods of educational and social science research: The logic of methods. (3rd ed.) Long Grove: Waveland Press.

Krueger, K. P., Russell, M. A., & Bischoff, J. (2011). A health policy course based on fink's taxonomy of significant learning. American Journal of Pharmaceutical Education, 75(1), 14.

Lawrence-Keuther, M. (2020, July 6). Personal communication.

Lee, W. C., & Lutz, B. D. (2016). An anchored open-ended survey approach in multiple case study analysis. Paper presented at the ASEE Annual Conference and Exposition, New Orleans, LA.

Miles, M. B., Huberman, A. M., & Saldana, J. (2020). Qualitative data analysis (4th ed.). SAGE Publications.

National Cyber Warfare Foundation. (2019) Cyber ranges. National Cyber Warfare Foundation. https://cwr.dev/ranges/

National Institute of Standards and Technology, (2018, August 27). NIST general information. NIST. https://www.nist.gov/National Institute of Standards and Technology. (2018, February 15). Cyber Ranges. NIST. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

Priyadarshini, I. (2019). Features and architecture of the modern cyber range: A qualitative analysis and survey. [Unpublished Master's thesis]. University of Delaware. http://dspace.udel.edu/bitstream/handle/19716/23789/Priyadarshini_udel_0060M_13323.pdf?sequence=1&isAllowed=y

Raymond, D. (n.d.) Using cyber ranges for cybersecurity education. Virginia Cyber Range. https://csrc.nist.gov/CSRC/media/Events/F ederal-Information-Systems-Security-Educators-As/documents/24.pdf

Saldana, J. (2016). The coding manual for qualitative researchers. SAGE Publications.

Smith, Jim III. (2017). Experiential learning via cyber ranges. National Institute of Standards and Technology (NIST) Federal Information Systems Security Educators' Association (FISSEA) Awareness – Training – Education. https://csrc.nist.gov/CSRC/media/Events/Federal-Information-Systems-Security-Educators-As/documents/6.pdf

Streveler, R. A., Smith, K.A., & Pilotte, M. (2012). Aligning course content, assessment, and delivery: Creating a context for outcome-based education. In K. M. Yusof, N. A. Azli, A. M. Konlin, S. K. S. Yusof, & Y. M.Yusof (Eds.), Outcome-based science, technology, engineering, and mathematics education: Innovative practices, 1-26. IGI Global.

Tracy, S. J. (2010). Qualitative quality: Eight "Big-Tent" criteria for excellent qualitative research. Qualitative Inquiry,16(10), 837-851.

Trochim, William M. (2006). The Research Methods Knowledge Base, 2nd Ed. at URL: http://www.socialresearchmethods.net/kb/.

Virginia Cyber Range. (n.d.) About. Virginia Cyber Range. https://www.virginiacyberrange.org/about

VMware. (2006). Virtualization overview: VMware white paper. VMware. https://www.vmware.com/pdf/virtualization.pdf

Yamin, M. M., Katt, B., & Gkioulos, V. (2019). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88. Elsevier.

Zippia Careers. (2021, December 14). Computer science teacher demographics. Retrieved March 10, 2022, from https://www.zippia.com/computer-science-teacher-jobs/demographics/#gender-statistics

Editor's Note:

This paper was selected for inclusion in the journal as an EDSIGCON 2022 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.

APPENDIX A
Cyber Ranges Providers, Participants, Stated Objectives, Infrastructure & Deployment

Cyber Range	Providers	Stated Objectives	Participants	Infrastructure Type	Deployment Type
University of Maine at Augusta	Academic	MDI, ED, E&C	All users	Public	Cloud & VPN
Virginia	Academic	ED	Students & Academic researchers	Public/Private	Cloud Only
Michigan	Academic	MDI, ED, E&C	All users	Federated/Public/Private	Cloud & VPN
University of Delaware	Academic	ED	All users	Private	No Cloud
Regent University	Academic	MDI, ED, E&C	All users	Private	Cloud & VPN
Wayne State	Academic	MDI, ED, E&C	All users	Federated/Public/Private	Cloud & VPN
Arkansas	Academic	ED	Students	Public	No Cloud
Georgia	Academic	MDI, ED, E&C	All users	Public/Private	Cloud & VPN
Cyber Warfare Range (Arizona)	Academic	OS	All users	Public/Private	Cloud & VPN
National (DARPA)	Government	MDI, ED, E&C	All users	Federated	Cloud & VPN
Department of Defense (DOD)	Government	MDI	Organizations & Professionals	Federated	Cloud & VPN
NATO	Government	MDI	Organizations	Federated	Cloud & VPN
IBM	Commercial	E&C	Organizations & Professionals	Private	Cloud Only
Cisco	Commercial	ED & E&C	All users	Public/Private	Cloud Only
Raytheon	Commercial	E&C	Organizations & Professionals	Federated	Cloud & VPN

Baltimore	Commercial	E&C	Organizations & Professionals	Public/Private	Cloud & VPN
Florida	Commercial	MDI, ED, E&C	All users	Federated/Public/Private	Cloud Only
Cyberbit	Commercial	SP	All users	Private	Cloud & VPN
Circadence	Commercial	SP	All users	Private	Cloud Only

(Abbreviations in Stated Objectives: **MDI**: Military, Defense, and Intelligence, **ED**: Education, **E&C**: Enterprise and Commercial, **SP**: Source Provided, **OS**: Open Source)

Providers_

The three types of providers are classified as government, commercial, and academic. Government providers include military, defense, and other government agencies. Commercial providers include industry related organizations, and academic providers include both private and public academic institutions.

Participants

Participants are cyber range users. These include organizations, professionals, students, and academic researchers.

Objectives

Several different utilization purposes were identified to classify cyber range operation objectives. The most common include the following Military, Defense, and Intelligence (MDI); Education (ED), Enterprise and Commercial (E&C), Source Provider (SP), and Open Source (OS).

MDI cyber ranges stated objective is to combat cyber terrorism and defend our national cyber-infrastructure. According to Davis and Magrath, the United States Air Force was a leader in cyber ranges, having used cyber ranges since 2002 (2013).

Priyadarshini claims the educational objective to utilize cyber ranges was more recently realized in 2015. Educational cyber ranges, EDs, meet educational needs for training, certification preparation, and research. However, Davis and Magrath cite earlier academic endeavors to simulate the effects of network attacks for training purposes to include University of Illinois' Real Time Immersive Network Simulation Environment (RINSE) in 2006 and Rochester Institute of Technology's ARENA simulation software in 2007 which modeled "computer networks and intrusion detection systems (IDS) and then applies simulated attacks" (2013, p. 9).

Organizations utilize E&C cyber ranges to not only train their employees, but to address vulnerabilities and threats to their digital infrastructure. IBM's cyber range, launched in 2016, is considered the first commercially available cyber range and uses live malware to test security (Priyadarshini, 2019).

Source providers offer cyber range solutions to meet various objectives. They offer simulation centers for training and testing services.

Finally, OS cyber ranges meet different objectives, to include training and testing for the various types of users. They differ from others in that they are open, free environments that encourage the users to contribute to the available resources to include war games and real opponent challenges.

Infrastructure Type

Three primary associations were identified for classifying based upon the type of infrastructure to include Federated, Private, and Public. These classifications are based upon funding support. Some cyber ranges belong to multiple infrastructure groups as they are supported through a collaborative effort of these types of organizations.

Deployment Platforms

Cyber Range variations can be broadly classified into four main platforms (Darwish et al., 2020; Raymond, D., n.d.) to meet the needs of its users. These types include Local Network Virtualizations, Hosted Virtualizations, commercial-hosted offerings, and Cloud-hosted offerings.

Local Network Virtualization (Raymond, D., n.d.) supports customization of the environment, through network virtualization software, to build various network models and labs for onsite training. These cyber ranges have limited scalability and require a significant financial investment not only for deployment on the site's infrastructure but additionally for the costs associated with ongoing maintenance and administrative support.

Hosted Virtualization (VMware, 2006) supports smaller environments. Virtualization software, such as VMWare or VirtualBox is used to create the training environment on the client machine. Although free virtualization software options exist, the client machine requirements to effectively run the virtualization adds considerable costs.

Commercial-hosted offerings support large and small learning environments. They provide courseware, labs, and pre-configured environments for students to access via a web portal. Most include registration fees based on the duration of registration time or upon specific course registration. The courseware tends to focus on industry certification preparation as they partner with various organizations to include Cisco, Palo Alto, and CompTIA.

Cloud-hosted offerings also support both large and small learning environments. They focus on cybersecurity academic support needs, providing courses, labs, workshops, videos, scenario simulation exercises, and both off-the-shelf (OTS) and customizable Capture the Flag (CTF) competitions (Beauchamp et al., 2020).

APPENDIX B
Anchored Open-Ended Questionnaire for Educators

Please provide the following information regarding your teaching experience and background. Complete one row for each course you have taught within the past five years. Please use the text box to provide the name of the specific course. Space is provided for up to six courses.

Course	Currently teaching or have taught this in an academic year?	Number of times teaching this subject in the past five years	If currently teaching, the number of students enrolled in this course across all sections you teach/taught during this academic year.	Average class size per section	Grade level (elem, middle, high, college)

1. Which of the following contributed to your preparation for teaching cybersecurity? Check all that apply.
   - Professional experience (Please state the type of profession and years of experience.)
   - Industry certifications (please list the certifications and year of acquisition)
   - Online workshops
   - Formal academic course(s) related to cybersecurity (please list the courses).
   - Virginia Department of Education license (please state your area(s) of licensure)
   - Community of Practice/Informal learning community(s) (Please list)
   - Other (please specify)
1. Have you used the Virginia Cyber Range in any capacity during the 2020 - 2021 academic year? If the response is no, skip questions of how used.

The Cyber Range in this questionnaire refers specifically to the Virginia Cyber Range.

1. Please select all that apply for how you use the cyber range for cybersecurity education and how often. Primary being it is your primary resource for that specific cybersecurity education area, i.e. homework or assessment tool.

Cyber Range Resource	**Class teaching and learning activity**	**Homework activity**	**Assessment tool**	**Professional Development**	**Enrichment/ Other use**
Hands-on laboratory exercise in an immersive environment	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Weekly Workshop Series	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Video lessons	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Capture the Flag (CTF) events	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all	Primary Secondary Barely Not at all

	N/A	N/A	N/A	N/A	N/A
Other Cyber Range Resource	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A
Community of Practice	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A	Primary Secondary Barely Not at all N/A

1. Please describe how you use the cyber range for enrichment and/or other use and the usage level for cybersecurity education: primary, secondary, or barely.
2. Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.
3. Please provide some specific examples of how you use the cyber range to support your assessment efforts.
4. Please provide some specific examples of how you use the cyber range to provide feedback to your students.
5. Please provide some specific examples of how you use the cyber range for teamwork and collaborative activities.
6. How often do you use the cyber range? (in the last year, how many hours, on average).
7. What percentage of your total cyber range usage do you utilize the following items?

    0. Hands-on Labs (List the three most used)

    1. Weekly Workshop Series

    2. Video Lessons

    3. CTFs

    4. Other cyber range resource (Please list them here)

    5. Community of Practice

2. What percentage of all the resources you utilize to teach cybersecurity education, does the cyber range contribute for the following items?

    0. Class teaching and learning activities

    1. Homework

    2. Assessment tool

    3. Professional development

    4. Enrichment/Other use

2. How do you describe your gender identity? Male, Female, Prefer to self-describe; below:
3. With which racial group(s) do you identify? (Mark all that apply) American Indian or Alaska Native; Hispanic, Latino, or Spanish origin; White; Black or African American; Asian; Middle Eastern or North African; Native Hawaiian or Other Pacific Islander; Another race or ethnicity not listed above:

APPENDIX C
Examples of the Coding Steps

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses
CyberSecurity 02 Ubuntu Linux - Bash Basics CyberSecurity 00 Windows 10 Lab CyberSecurity 01 Kali-Linux Lab Laboratory exercise: Cyber Basics - Introduction to the Linux Terminal and Understanding Directories	Cybersecurity lessons for Linux - Bash Basics, Windows 10, and Kali-Linux to intro to Linux terminal and understanding directories.
- An entire unit on Command Line Interface (Linux) to get familiar with the command line. - Lab and assignments using mcrypt in Linux when teaching about encryption - Lab and assignments using John the Ripper when teaching about hashing/passwords/authentication - Lab using ifconfig, nmap, nslookup, dig, when teaching about Networking Basics - Lab and assignment on Windows password, account lockout and user rights assignment settings when teaching about Data & Network Defense - Lab and assignment in both Linux and Windows when teaching about users, groups, and share permissions in a unit on User Security	Linux environment and tools such as John the Ripper, nmap, nslookup, network defense concepts, users/groups permission settings for User security concepts
In CS 2104 we have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking).	CTF challenges
We use the Cyber Basics environment for the Linux Machine. Additionally, we use the CTF activities for fun additional practice, as well as for demonstrative purposes.	Linux Machine and CTF for practice and demonstration
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.

Appendix Table B1: Summary Ideas of the Usage of the Cyber Range to Support Cybersecurity Educator Teaching and Learning Activities

Please provide some specific examples of how you use the cyber range to support your teaching and learning activities.	Summary ideas from the responses	Codes from the summary ideas
For example, we have used lessons regarding the understanding and use of the Kali Linux command line this week. Guided exercises that work are engaging to the students--much more than the vocabulary driven work we have in the textbook.	Supports hands-on application of concepts, such as Kali Linux command line practice versus textbook vocab memorization.	hands-on application labs
After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment.	Used CTF related problems to the current technical content as a supporting/reinforcing assignment.	labs reinforce lessons CTF
I use the cyber range as a hosting environment for cybersecurity labs and to pull from content. Our textbook (Principles of Cybersecurity) does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap.	Use to support textbook content by using the VaCR labs/environment	labs accessible environment

Appendix Table B2: Initial Codes of How Educators Used the VaCR for Their Cybersecurity Teaching and Learning Activities

Hands-on Practice	Existing Labs and Lessons	CTFs	Safe and Accessible Environment
demonstrate learning	Linux	CTFs	VM
hands-on application	Labs for homework	CTF preparation	VM - safe environment
practical application	Lab assignments	CTF - homework	supplemental environment
hands-on practice reinforce learning	Labs reinforce lessons	CTF - group assignments	supplemental environment - supports textbook labs
	Labs aligned with LOs	CTFs, summer camps, and Cyberpatriot - team effort	supplemental environment - support use of third party tools
	Labs - extra credit	CTF - teamwork	supplemental environment - hacking tools
	Outreach support	CTF - team SMEs	Safe sandbox

Appendix Table B3 Themes and their Supporting Codes for How Cyber Ranges are Used for Teaching and Learning Activities

APPENDIX D
Academic Courses Taught by VaCR Registered Educators

High School Courses	Community College Courses	University/College Courses
Accounting, Econ and Personal Finance, & Marketing	CompTIA A+ certification	Breach Remediation
Prob/Stats & Discrete Math	CompTIA Security+ preparation	Computer Networks
AP Physics 1, IB Physics SL, & Physics	Computer Crimes and Hacking	Cyber Forensics
Adv Cybersecurity Software Operations	CSC 200 Intro Comp Sci	Cyber Security II
Adv Cybersecurity Systems Technology	CSC 201 - Computer Science I	Intro to Cybersecurity
Advanced Information Systems	CSC 205 - Computer Organization	Intro to Digital Forensics
Cisco	IT 106 Microcomp OS	Intro to Problem Solving in CS
Computer Network Software Operations	ITD 130 Database Software	Securing the Cyber World
Computer Systems Technology I	ITE 115 Micro Comp Software	Strategic Management
Cybersecurity Fundamentals and Advanced	ITE 130 - Internet Services	Strategy Competition Analytics
Cybersecurity Network Systems	ITE 140 Adv Spreadsheeting	
Cybersecurity Software Operations	ITN 101 Introduction to Network Concepts	
Cybersecurity Systems Technology and Advanced	ITN 170 Linux Sys Admin	
Game Design and Advanced	ITN 171 UNIX	
Hardware and Networking	ITN 200 Administration of Network Resources	
Information Systems	ITN 260 Intro Network Security	
Intro to CS with Python	ITN 275 Incident Response and Computer Forensics	
Introduction to Computer Science	ITN-262: Network Comm, Security & Authentication	
Intro to Programming	ITP 100 Software Design	
IT Fundamentals	ITP 120 Java	
M284 Adv Programming	ITP 270 Programming for Cybersecurity	
M286 Intermed Programming		

M288 AP Computer Science Principles		
Network+		

APPENDIX E
Educator Excerpts Regarding Teaching and Learning Activities Using the VaCR

Accessible Environment	*"We compete in the National Cyber League. Some of the challenges require tools that are installed on Kali Linux, so the VACR Kali image is excellent. Students don't have to download and install Kali. Of those students that have VMware, several do not have enough disk space to have multiple VMs." [Experienced, Community College]* *"I use the cyber range as a hosting environment for cybersecurity labs." [Experienced, High School]*
Hands-on Application & Practice	*"Being able to use the virtual machines online has been amazing. We use them to practice Windows management, which would normally be blocked, learn terminal/command line, and cybersecurity exercises."[Experienced, High School]* *"Use cyber range environments for application of network reconnaissance, footprinting, enumeration principles, firewall and IDS configuration principles, and for public key cryptography concepts." [Experienced, College]*
Existing Labs & Lessons	*"Our textbook does not currently have a lab manual that is worth using (outdated and no live environment) the cyber range fills that gap." [Experienced, High School]* *"Some of the labs provided by the publisher do not directly map to specific learning objectives for the course so I identified more appropriate ones in the range." [Experienced, College]*
CTFs	*"After each lesson on a technical subject I often assign one of the existing problems in the CloudCTF related to it as a supporting/reinforcing assignment." [Experienced, High School]* *"We have three CTF group-based classwork assignments where, for each, students attempt to solve challenges in a specific domain (web reconnaissance, cryptography, networking). [Experienced, College]*

APPENDIX F
Educator Excerpts Regarding Feedback and Assessments Using the VaCR

Formative Assessment	*"Using the cyber range gives students the opportunity to ask questions about something they maybe didn't fully grasp before." [Novice, High School]* *"I use the labs given via the range or cyber.org to help them better understand where their weaknesses are and what they need to improve on." [Experience, Community College]*
Summative Assessment	*"Assessments are based on successful completion of tasks assigned directly relating back to course competencies." [Novice, High School]* *"I sometimes write CTF problems as "quiz" problems, which serve as self-grading activities." [Experienced, High School]*
Feedback	*"I ask my students if they like the labs and what their favorite part is." [Novice, High School]* *"Students will be assigned specific tasks, most recently account management policy via Windows Local Security Policy. Each student needed to properly configure the settings, as outlined in the assessment. I logged into each machine to verify settings and give feedback." [Experienced, Community College]*

A Survey of Privacy Metrics for Smart Homes

Nooredin (Noory) Etezady
netezady@unm.edu
Anderson School of Management
University of New Mexico
Albuquerque, NM, USA

Abstract

Internet of Things (IoT) has exponentially increased the collection of different types of consumer information through IoT sensors. IoT makes people's life more convenient and at the same time poses new challenges to privacy and security protection. Most consumers do not completely realize the potential privacy and security risks related to IoT. To make the matters worse, there is no standard metric for IoT and specifically for smart homes. There have been several calls by researchers for identification and development of new metrics to measure the level of privacy harm and security protection. In this paper a comprehensive literature review was conducted on privacy metrics for smart homes. A total of 69 papers were identified. Three papers specifically addressed smart homes privacy and privacy metrics. The metrics developed by these papers have their shortcomings and need to be further verified and tested.

Keywords: smart home, privacy, metric, IoT, Internet of Things

1. INTRODUCTION

Internet of Things (IoT) has exponentially increased the collection of consumers' information through device sensors. Although IoT makes people's life more convenient, at the same time it poses new challenges to privacy and security protection. Most consumers do not completely realize the potential privacy and security risks related to IoT (Choi, Lowey, & Wang, 2020).

Access control and cryptography for controlling privacy have been researched with strong results. These methods can be strong deterrents against outside adversaries. However, they do not provide privacy protection against those with access to the data (Dong, Ratliff, Cardenas, Ohlsson, & Sastry, 2018). For example, utility companies with access to energy consumption may be able to infer lifestyle information from usage patterns.

One of the prime factors for users' willingness to deploy smart technology is convenience. However, it appears that personal data tracking by these devices is not important to the users of these technology (Princi & Kramer, 2020). Choi et al. (2020) noted that many consumers have limited information on IoT and even the ones with enough information seldom protect their personal information because of the cognitive gap between the attitude and actual behavior.

Although IoT maximizes convenience, the unseen collection of data, usage, and sharing increase privacy concerns for IoT users (Aleisa & Renaud, 2017). IoT privacy and security problems intensify the demand for mechanisms to protect IoT privacy and security (Choi et al., 2020).

As Amar, Haddadi, and Mortier (2018) noted; users are usually oblivious to the kind of information they are divulging. The users' data patterns can be used for inference and the users cannot be expected to be aware of that. Zheng, Apthorpe, Chetty, and Feamser (2018) also stated that users need to be informed of the continuing data collection through IoT devices. In most cases, collection of some type of data might be harmless. However, specific household information can lead to compromising inferences.

They also observed that for privacy protection, it is necessary to make it easier for the users to understand and control smart home data collection. Providing a way to easily configure privacy features would assist users with privacy protection. Privacy metrics will assist users in understanding the level of privacy protection of their devices and motivate them to configure their privacy features.

The contribution of this paper is to present an overview of the existing research on smart homes (IoT for homes) privacy metrics and to point out its shortcomings.

2. LITERATURE REVIEW

In general, research on identifying metrics for privacy has been scarce. Research by Liu and Terzi (2010) is one of the exceptions who developed a framework for computing privacy scores for online social networks users. There have been calls by several researchers for identifying privacy metrics (Bugeja, Jacobsson, & Davidsson, 2020 ; Vemou & Karyda, 2018; Haug, Lanza, & Gewald, 2021).

Research on IoT privacy metrics is also scarce. Choi et al. (2020) noted that many previous privacy scoring studies are on the context of social media. Therefore, the IoT vulnerabilities and new information types used in IoT are not considered.

Toch, Bettini, Shmueli, Radaelli, Lanzi, Riboni, and Lepri (2018) called for the identification and development of new metrics that measure the level of privacy harm and security protection of systems. These new metrics could help in the future development and regulation policies of cyber security systems.

Various researchers have suggested different ways to measure privacy. For example, Haug et al. (2021) stated that to measure privacy concerns one might need to utilize privacy risks as a proxy. Bugeja et al. (2020) presented a data sensitivity metric based on personal data exposure for smart connected homes. Dong et al. (2018) looked into the behavioral methods and noted that since it is not easy to convert a person’s emotions and decision making about privacy into a mathematical object, the majority of existing behavioral methods can be useful. Using behavioral methods requires emphasis on a privacy level evaluation that closely follows either a person’s privacy assessment or decision to reveal information. User studies research that employ this method will maintain their applicability to real-life applications.

Machine learning can also be utilized in privacy research. Liu, Ding, Shaham, Rahayu, Farokhi, and Lin (2021) noted that machine learning can be used as a powerful tool for privacy research from an attack as well as defense point of view.

There are several literature review papers on IoT and smart homes privacy concerns (Abdi, Zhan, Ramokapane, & Such, 2021; Aleisa & Renaud, 2017; Kulyk, Milanovic, & Pitt, 2020; Ogonji, Okeyo, & Wafula, 2020; Princi & Kramer, 2020; Yao, Basdeo, McDonough, & Wang, 2019). However, as of the date of this paper, no literature reviews on privacy metrics for smart homes were found.

This study is a literature review of privacy metrics for smart homes. The results of this study will help researchers to understand the current status of research on smart home privacy metrics and the need to develop privacy metrics for smart homes.

3. METHOD

The methodology developed by Pickering and Byrne (2014) was used in order to systematically analyze existing academic literature and produce a quantitative overview of smart-home privacy metrics. The benefit of this method is its facility for finding what the existing research covers and where the gaps are (Aleisa & Renaud, 2017). This method has been used by various researchers in the past (Aleisa & Renaud; Ogonji et al., 2020; Low-Choy, Riley, & Alston-Knox, 2017; Templier & Pare, 2018; Bergstrom, Van Winsen, & Henriqson, 2015).

The Pickering and Byrne (2014) methodology is a 15-stage process that starts with defining the topic, formulating research questions, identifying keywords, identifying and searching databases to evaluating key results and conclusions and finally revising paper until it is ready for submission. See figure 1 in appendix B.

Webster and Watson (2002) noted that leading journals are likely to be the major contributors. They further recommended examining reputable conference proceedings and to go backward by reviewing the citations of the identified articles to determine prior articles that need to be included. Based on Webster and Watson’s recommendation, the following databases were searched for research papers and conference proceedings related to Home IoT privacy metric:

Association of Information systems (AIS), ACM, IEEE Xplore, Elsevier ScienceDirect, ProQuest, Emerald Management, and Web of Science. Only research in English was considered. Considering that 70% of social science and 90% of natural science research is conducted in English the language bias may not be large (Pickering & Bryne, 2014).

A combination of the following keywords was used: Internet of Things, IoT, home, Smart Home, Privacy metric, and privacy measurement. The search was conducted up to and including the year 2022.

Databases	Number of Articles
ACM	10
AIS	10
Elsevier Science Direct	18 (The total was 41. Only 18 papers were relevant to IoT after reading the abstracts.)
Emerald Management	1
IEEE	13
ProQuest	16
Web of Science	1
Total:	69 (92 total)

Table 1: Search Databases 1

4. RESULTS

The search yielded 92 original peer-reviewed research papers. The abstract, methodology, and conclusion of these papers were reviewed to identify the ones addressing privacy for internet of things. There were 69 papers that discussed privacy specifically in the IoT domain. Research on IoT privacy was categorized among various IoT research areas as shown in table 2.

The top three area of IoT privacy research were Location Based Services (LBS) with 13 papers; followed by IoT privacy models, frameworks, and protocols with 12 papers; and healthcare with 5 papers. Since locations-based services are used by smart devices and applications (for example; smart phones, smart vehicles, and web applications) user privacy is a major concern, which is reflected by the number of research papers in that area. To implement privacy; privacy models, frameworks, and protocols are needed; which explains the high number of research papers on the topic. Healthcare data, such as patient data, needs to be safeguarded. Patients' privacy is also of prime concern shown by the number of research papers on healthcare privacy.

There has been less research on smart homes privacy as it is a relatively new area for IoT and of less importance compared to the top three. However, as indicated in table 2 by the low number of research papers on smart homes privacy, more research is needed on smart homes privacy. In general table 2 is a good indicator for the IoT privacy research areas that need attention.

IoT Area	Number of Papers
Camera Glass	1
Crowdsourcing	2
Cyber-physical Systems	3
Data (utility & privacy)	1
Data – Car	1
Data – Personal	3
Healthcare	5
IoT & privacy models, frameworks, and protocols	12
Location Based Services (LBS)	13
Machine Learning	1
Mobile Analytics on IoT Devices	1
Mobile applications used in smart homes & IoT devices	1
Mobile participatory sensing*	1
Network Monitoring (IoT)	1
Privacy labeling	1
Privacy preserving solutions	1
Smart Cities - Crowdsensing	1
Smart Communities	1
Smart Devices	1
Smart Devices – mobility management	1
Smart Energy Management Systems	1
Smart Grid	3
Smart Home	3
Smart Home - Speakers	2
Smart Meter	2
Value Creation in IoT (Digital Platform) Eco-system	1
Vehicles	4
Wearables	1
Total	69

Table 2: IoT Privacy Research Categories

Various aspects of privacy were addressed by the reviewed research papers. Some researchers investigated personal data privacy for any system that obtains personal data. One such example is Amar et al. (2018) that studied personal data privacy for any system that data consumers use to obtain personal data. They suggested implementing personal data privacy for producers of data using cheap hardware at the source of data. Other researchers like Dong et al. (2018) investigated the tradeoff between stringent data privacy rules and usefulness of the obtained data for consumers of that data.

*In table 2, mobile participatory sensing refers to the sensing, processing, and storage resources in mobile phones that is used to obtain insight about the participants and their environment through various applications (Christin, 2016).

To identify research that specifically addressed privacy metrics; the introduction, methodology, and conclusion of the 69 research papers in table 2 were read carefully. In some cases, the whole paper was read. Eighteen research papers were identified that discussed privacy metrics in IoT. These research papers are listed in table 3 in Appendix A. The findings from table 3 are discussed in the next section.

5. FINDINGS

The privacy metrics, models, or frameworks that were discussed or developed in the reviewed papers were mostly based on one or more of three main privacy metrics. These privacy metrics included differential privacy, k-anonymity, and entropy and have been used by various researchers in the past.

Differential privacy was first introduced and used in statistic databases. It is a rigorous mathematical definition of privacy. Differential privacy was inspired by Dalenius (1977) that "nothing about an individual should be learnable from the database that cannot be learned without access to the database" (Dwork, 2006). In simple terms, differential privacy introduces noise into a dataset so that personal information cannot be identified when statistical analysis is performed on the dataset.

As Dong et al. (2018) noted, the most popular privacy metric is differential privacy. However, differential privacy for many practical applications requires a particular structure of uncertainty. Its use is not clear in a dynamic system when the sampling rate is adjusted (Dong, et al.).

k-Anonymity is a widely adopted method for preserving privacy that was introduced for the database community by Sweeney (2002). K-anonymity is based on hiding sensitive information by introducing k-1 dummies so that the adversary will be unable to recognize the actual information.

Entropy was first introduced by Serjantov and Denezis (2002) to measure the degree of uncertainty in an anonymous set. Entropy privacy metric refers to the uncertainty in a random variable. Entropy is the measure of anonymity in a set (Babaghayou, Labraoui, Abba Ari, Lagraa, & Ferrag, 2020). A lower entropy translates into a lower privacy protection level (Alaradi and Innab, 2019). Entropy is used in Location Based Services (LBS) to measure the uncertainty degree of a location belonging to a user (Sun, Chen, Hu, Qian, & Hassan, 2017).

Cyber-physical Systems

To protect user's privacy in smart cyber-physical systems Chaaya, Barhamgi, Chbeir, Arnould, & Benslimane (2019) proposed Privacy Oracle. Privacy Oracle is a context-aware semantic reasoning system, providing users with a dynamic overview of their privacy risks as their context changes. When users are aware of the direct and indirect privacy risks, they can take the proper steps to protect their privacy.

Location Based Services (LBS)

Compromised location servers, which store users' activities information, can use inference attacks to track the users' real location and obtain personal and sensitive user information. Alaradi and Innab (2019) proposed Location Based Services protection method to guarantee location privacy by enhancing the previously employed method of using dummy locations. Dummy locations surround the real location to impede recognition of the real location among the dummies by the server. Alaradi and Innab employed entropy privacy metric.

Set of Anonymity Size (SAS) "refers to the indistinguishability of a target vehicle in comparing to other vehicles in the same context." (Babaghayou et al., 2020). Babaghayou et al. surveyed the Vehicular Ad-hoc Networks (VANETS) privacy protection strategies that use pseudonyms in place of individual real identities and changing them often to protect the privacy of users. They reviewed various location based privacy metrics for VANETS, including SAS, entropy, the degree of anonymity, adversary's success rate, maximum tracking time, and statistics on pseudonym change. Babaghayou, Labraoui, Abba Ari, Ferrag, Maglaras, and Janicke (2021) used a location privacy metric called traceability. Traceability is defined "as the correctness of an adversary to build the target vehicle's traces using eavesdropped beacons" (Babaghayou et al., 2021).

Bin, Lei, and Guoyin (2019) proposed a mathematically rigorous method for LBS privacy protection called ε-sensitive correlation privacy protection scheme which provides correlation indistinguishable to the location data. Entropy is used in Ɛ-sensitive correlation privacy protection.

IoT

Consumer-disclosed information is classified by previous research into six information types, which include demographic; contact; vehicle; lifestyle, interests, and activities data; financial and economic data; and financial and credit data. Examples of financial and economic data include estimated income and home value. Examples of financial and credit data are credit score, loan, and credit card data. The new type of data that is captured by IoT includes consumers' behavioral tendencies, real-time locations, and schedules, which can be subject to ill use (Choi et al., 2020).

To protect private information of IoT users, Choi et al. (2020) proposed a design framework to evaluate and quantify IoT privacy security risks (PSR) that is associated with IoT adoption. PSR scores are used to assess IoT Privacy and Security Risks (PSR). PSR scores are determined by the collective consideration of consumers' IoT information types, weight impact factors, and personal capabilities. Their work contributes to increasing user awareness of PSRs and thereby minimizing the cognitive gap that is the possible cause of consumers' paradoxical behaviors when it comes to protecting their privacy. The limitation of the proposed approach is that the direct impact of cognitive gap between the attitude and actual behavior is not easily measurable. In addition, PSR scores can be subjective until there are sufficient PSR scores to compare individuals to populations. And finally, the individuals' personalities and experiences change in different cultures which affects risks associated with different information types (Choi et al.).

Dong et al. (2018) introduced inferential privacy metric for IoT that takes into consideration data quality and its utility to the collectors of data. Inferential privacy metric is the probability that an adversary can correctly infer private information from public observations. However, in practice, determining the required distributions is not trivial (p. 9).

Tavakolan and Faridi (2020) presented a model for describing and applying privacy-aware policies in IoT devices. They suggested dividing general privacy policies into four main metric categories of obligation, disclosure, collection, and selectivity that could be used to build a descriptive model of privacy aware policy on IoT devices. These general categories can be further expanded into more metric subcategories. The proposed model needs to be evaluated and tested practically.

Smart Energy Management Systems

Ukil, Bandyopadhyay, and Pal (2015) proposed a privacy management method for smart energy applications. The proposed approach automatically detects, measures, and preserves privacy for smart meter data before sharing it with third parties. The user will also be alerted when there is a possibility for privacy breaches of the shareable data. The proposed method requires a facilitation tool or device to perform the necessary analysis and computation on data.

Smart Homes

Bugeja et al. (2020) classified smart connected home systems into a four-tiered classification of app-based accessors, watchers, location harvesters, and listeners. An equation was then presented to calculate the data sensitivity score of smart home systems. Data type (e.g., Image, audio, position), privacy parameter (e.g., data type sensitivity, location sensitivity, and data accessibility) were used in the equation to calculate data sensitivity score. It is possible to include other parameters such as data retention time and trust in a manufacturer to measure data sensitivity. The proposed data sensitivity metric needs to be analyzed and validated. A metric will also be needed for grading the calculated data sensitivity.

Daubert, Wiesmaier, and Kikiras (2015) proposed a model that linked information, privacy and trust. The model was based on privacy dimensions and trust dimensions. Privacy dimensions included identity privacy, location privacy, footprint privacy (such as preferred language and operating system), and query privacy (e.g., the fact that a query is made on weather). Trust dimensions included trust in device, processing, connection, and system.

Kennedy, Li, Wang, Liu, Wang, and Sun (2019) proposed a new privacy metric for voice command fingerprinting attacks against smart-home speakers called semantic distance that used natural language processing to measure the privacy leakage. A voice command fingerprinting attack takes advantage of the fact that every voice command and its response, although encrypted, possess a unique traffic pattern because of packet length, direction, order, etc. (Kennedy et al., 2019). The semantic distance metric uses accuracy, which is the effectiveness of a voice command fingerprinting attack, and semantic distance. Semantic distance refers to the fact that two similar voice commands are not exactly the same, for example "what is the weather" and "what is the weather tomorrow?". Semantic distance is used as a metric to measure privacy leakage in addition to accuracy.

6. CONCLUSION

With the progressive advancement of technology, Internet of Things (IoT) has exponentially increased the collection of numerous consumers' information through IoT sensors. IoT makes people's life more convenient and at the same time it confronts them with new challenges to privacy and security protection. Research shows that most consumers do not completely realize the potential privacy and security risks related to IoT (Choi et al., 2020).

There is no standard metric for smart homes. Several researchers have called for identification and development of new metrics to measure the level of privacy harm and security protection (Bugeja et al., 2020; Toch et al., 2018; Haug et al., 2021; Vemou & Karyda, 2018). Development of new metrics could also help in the future development and regulation policies of cyber security systems.

In this paper a comprehensive literature review was conducted on privacy metrics for smart homes. From a total of 69 papers that were identified, only three research papers by Bugeja et al. (2020), Daubert et al. (2015), and Kennedy et al. (2019) addressed smart homes privacy and privacy metrics. The metrics developed by these papers have their shortcomings and need to be further verified and tested.

Considering the dearth of research on IoT and smart home privacy, future researchers need to focus on identifying and developing new metrics for IoT and smart homes as a step toward user privacy protection.

7. REFERENCES

Abdi, N., Zhan, X., Ramokapane, K. M., & Such, J. (2021). Privacy norms for smart home personal assistants. *Proceedings of the ACM CHI Conference, Yokohama*, 14 pages.

Alaradi, S., & Innab, N. (2019). Ensuring privacy protection in location-based services through integration of cache and dummies*. International Journal of Advanced Computer Science and Applications (IJACSA). 10*(2), 88-100.

Aleisa, N., & Renaud, K. (2017). Privacy of the Internet of Things: A systematic literature review. *Proceedings of the 50th Hawaii International Conference on Systems Sciences*, 5947-5956.

Amar, Y., Haddadi, H., & Mortier, R. (2018). An Information-Theoretic Approach to Time-Series Data Privacy. *Proceedings of InW-P2DS'18: 1stWorkshop on Privacy by Design in Distributed Systems, April 23–26, 2018, Porto, Portugal. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3195258.3195261*

Babaghayou, M., Labraoui, N., Abba Ari, A. A., Lagraa, N., Ferrag, M. A. (2020). Pseudonym change-based privacy-preserving schemes in vehicular ad-hoc networks: a survey. *Journal of Information Security and Applications. 55* (2020) 102618, 1-17.

Babaghayou, M., Labraoui, N., Abba Ari, A. A., Ferrag, M. A., Maglaras, L., & Janicke, H. (2021). WHISPER: A location privacy-preserving scheme using transmission range changing for Internet of Vehicles. *Sensors, 21*,2443,1-21.

Bansal, G., & Nah, F. (2020). Measuring privacy concerns with government surveillance and right-to-be-forgotten in nomological net of trust and willingness-to-share. *Proceedings of American Conference on Information Systems*, 1-10. 31.

Beker, I., Posner, R., Islam, T., Ekblom, P., Borrion, H., McGuire, M., & Li, S. (2021). Privacy in transport? Exploring perceptions of location privacy through user segmentation. *Proceedings of the 54th Hawaii International Conference on Systems Sciences.* 5347-5356. URI:https://hdl.handle.net/10125/71270. 978-0-9981331-4-0

Bergstrom, J., Van Winsen, & R., Henriqson, E. (2015). On the rationale of resilience in the domain of safety: a literature review. *Reliability Engineering & System Safety, 14*, 131-141.

Bin, W., Lei, Z., & Guoyin, Z (2019). A novel Ɛ-sensitive correlation indistinguishable scheme for publishing location data. *PLoS ONE, 14*(12), 1-17.

Bugeja, J., Jacobsson, A., &Davidsson, P. (2020). Is your home becoming a spy? A data-centered analysis and classification of smart connected home systems. *Proceedings of the 10th International Conference on the Internet of Things (IoT 2020), Malmo, Sweden.* ACM, New York, USA, 8 pages.

Chaaya, K. B., Barhamgi, M., Chbeir, R., Arnould, P., & Benslimane, D. (2019). Context-aware system for dynamic privacy risk inference, Application to smart IoT environments. *Future Generation Computer Systems. 101*, (2019),1096-1111.

Choi, D., Lowry, P. B., & Wang, G. A. (2020). The design of personal privacy and security risk scores for minimizing consumers' cognitive gaps in IoT settings. *Proceedings of the 53rd Hawaii International Conference on Systems Sciences.* 5076-5085.

Christin, D. (2016). Privacy in mobile participatory sensing: Current trends and future challenges. *The Journal of Systems and Software 116*(2016), 57-68.

Dalenius, T. (1977). Towards a methodology for statistical disclosure control. *Statistik Tidskrift 15*, pp. 429–222.

Daubert, J., Wiesmaier, A., & Kikiras, P. (2015). A view on privacy & trust in IoT. Proceedings of IEEE ICC 2015 - Workshop on Security and Privacy for Internet of Things and Cyber-Physical Systems. 2665-2670

Dong, R., Ratliff, L. J., Cárdenas, A. A., Ohlsson, H., & Sastry, S. S. (2018). Quantifying the Utility–Privacy Tradeoff in the Internet of Things. *ACM Trans. Cyber-Phys. Syst. 2, 2, Article 8 (May 2018), 28 pages. https://doi.org/10.1145/3185511*

Du, Y., Cai, G., Zhang, X., Liu, T., & Jiang, J. (2019). An efficient dummy-based location privacy-preserving scheme for Internet of Things services. *Information 2019, 10*, 278. 1-15.

Dwork, C. (2006). Differential privacy. *Proceedings of the International Colloquium on Automata, Languages and Programming*. Springer, 1–12.

Haug, M., Lanza, J., & Gewald, H. (2021). Only if it affects me! The influence of privacy on different adoption phases. *Proceedings of the Forty-Second International Conference on Information Systems (ICIS 2021), Austin.*10. 1-17.

Kennedy, S., Li, H., Wang, C., Liu, H., Wang, B., & Sun, W. (2019). I can hear your Alexa: Voice command fingerprinting on smart home speakers. *Proceedings of 2019 IEEE Conference on Communications and Network Security (CNS)*. 232-240.

Kulyk, O., Milanovic, K., & Pitt, J. (2020). Does my smart device provider care about my privacy? Investigating trust factors and user attitudes in IoT systems. *Proceedings of the 11th Nordic Conference on Human-Computer Interaction (NordiCHI '20)*, Tallinn, Estonia, 12 pages.

Li, T., He, X., Jiang, S., & Liu, J. (2022). A survey of privacy-preserving offloading methods in mobile-edge computing. *Journal of Network and Computer Applications, 203*, 103395, 1-28.

Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., & Lin, Z. (2021). When machine learning meets privacy: A survey and outlook. *ACM Computing Surveys, 54*(2), Article 31, 1-36. https://doi.org/10.1145/3436755

Liu, K., Terzi, E. (2010). A framework for computing the privacy score of users in online social networks. *ACM Transactions Knowledge Discovery from Data 5*(1), article 6, 1-30.

Low-Choy, S., Riley, T., Alston-Knox, C. (2017). Using Bayesian statistical modelling as a bridge between quantitative and qualitative analyses: illustrated via analysis of an online teaching tool. Educational Media International 54(4), 317-359.

Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. Computer Science Review, 38(2020), 100312, 1-19.

Pickering, C., & Byrne, J. (2014). The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers, *Higher Education Research & Development,* 33:3, 534-548, DOI: 10.1080/07294360.2013.841651

Princi, E., & Kramer, N. C. (2020). I spy with my little sensor eye – effect of data-tracking and convenience on the intention to use smart technology. *Proceedings of the 53rd Hawaii International Conference on System Sciences,* 1391-1400.

Serjantov, A., Danezis, G. (2002). Towards an information theoretic metric for anonymity. *In Privacy Enhancing Technologies*; LNCS 2482, Springer-Verlag Berlin Heidelberg 2003; pp. 41–53.

Sun, Y., Chen, M., Hu, L., Qian, Y., & Hassan, M. M. (2017). ASA: Against statistical attacks for privacy-aware users in location based service. *Future Generation Computer Systems. 70* (2017) 48-58.

Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), pp. 557–570.

Tavakolan, M., Faridi, I. A. (2020). Applying privacy-aware policies in IoT Devices using privacy metric. *International Conference on Communications, Computing, Cybersecurity, and informatics (CCCI)*. 978-1-7281-7315-3/20/

Templier, M., Paré, G. (2018) Transparency in literature reviews: an assessment of reporting practices across review types and genres in top IS journals. *European Journal of Information Systems 27*(5), 503-550.

Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., & Lepri, B. (2018). The privacy implications of cyber security systems: A technological survey. *ACM Comput. Surv. 51(2)*, Article 36, 1-27.

Ukil, A., Bandyopadhyay, S., & Pal, A. (2015). Privacy for IoT: Involuntary privacy enablement for smart energy systems. *Proceedings of ICC 2015 SAC - Internet of Things.* 536-541.

Vemou, K., & Karyda, M. (2018). An evaluation framework for privacy impact assessment methods. *Proceedings of the Mediterranean Conference on Information Systems (MCIS 2018),* 5. 1-10.

Wang, D., Ren, J., Wang, Z., Zhang, Y., & Shen, X. (2022). PrivStream: A privacy-preserving inference framework on IoT streaming Data at the edge. *Information Fusion, 80* (2022). 282-294.

Wang, J., Tian, L., Huang, Y., Yang, D., & Gao, H. (2018). Achieving the optimal k-anonymity for content privacy in interactive cyberphysical systems. *Security and Communication Networks. 2018*. Article ID 7963163. 1-15.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), xiii-xxiii.

Yao, Y., Basdeo, J. R., McDonough, O. R., & Wang, Y. (2019). Privacy perceptions and designs of bystanders in smart homes. *Proceedings of ACM Human-Computer Interaction, 3*(59), 1-24.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of Hum.-Comput. Interact.* 2, CSCW, Article 200, 20 pages.

Zhang, B., Liu, C. H., Lu, J., Song, Z., Ren, Z., & Ma, J. (2016). Privacy-preserving QoI-aware participant coordination for mobile crowdsourcing. *Computer Networks, 101*, 29-41.

APPENDIX A
Table 3

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
Zhang, Liu, Lu, Song, Ren, & Ma (2016)	Crowdsourcing - IoT Mobile Crowdsourcing	Entropy	Privacy-preserving participant coordination mechanism is proposed to achieve optimal Quality of Information (QoI) for sensing tasks and protect the participants' location privacy.	Elsevier
Wang, Tian, Huang, Yang, & Gao (2018)	Cyber physical systems	entropy and differential privacy	Proposed and used theoretical multilayer Alignment (MLA) algorithm to establish k-anonymity based mechanism for preserving privacy and to achieve content privacy	Prorequest
Chaaya, Barhamgi, Chbeir, Arnould, & Benslimane (2019)	Cyber physical systems	Privacy risk	Privacy Oracle - a context aware semantic reasoning system	Elsevier
Dong, Ratliff, Cardenas, Ohlsson, & Sastry, (2018)	Data - utility & privacy in IoT and smart grid	Inferential privacy	Inferential privacy	ACM
Babaghayou, Labraoui, Abba Ari, Ferrag, Maglaras, & Janicke. (2021)	Internet of Vehicles	location privacy metric called traceability.	WHISPER – A privacy preserving scheme based on reducing the transmission range while sending the safety beacons	Prorequest
Babaghayou, Labraoui, Abba Ari, Lagraa, & Ferrag (2020).	Internet of Vehicles - Vehicular ad-hoc networks (VANETS)	Reviewed LBS privacy metrics: SAS, entropy, the degree of anonymity, adversary's success rate, maximum tracking time, statistics of pseudonym change	Literature Review - A survey of various privacy protections based on pseudonym change strategies	Elsevier
Li, He, Jiang, & Liu (2022)	IoT	Privacy metrics for offloading: privacy entropy, task sensitivity, secrecy rate, secrecy outage probability, location privacy loss, and differential privacy	Literature review - Review paper on Edge Servers & wireless Transmissions (offloading).	Elsevier
Tavakolan & Faridi (2020)	IoT - A model for applying	Four main categories of obligation,	Users prioritize a set of extendable privacy policies by assigning	IEEE

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
	user preferences	disclosure, collection, and selectivity.	weights to the policies. The proposed method is used to apply user’s preferences within the privacy aware policies in IoT devices.	
Wang, Ren, Wang, Zhang, & Shen (2022)	IoT - Privacy preserving IoT streaming data analytical Framework (theoretical), based on edge computing	Sensitive inferences accuracy. Identity and gender recognition were defined as sensitive inferences.	It uses a deep learning model to filter sensitive information and combines with differential privacy to stop the untrusted edge server from making inferences from the IoT streaming data.	Elsevier
Choi, Lowry, & Wang (2020)	IoT - framework	Framework – The framework is grounded in cognitive dissonance theory and information processing theory.	A design framework for evaluating and quantifying IoT privacy security risks associated to IoT adoption	AIS
Alaradi & Innab (2019)	LBS (Location Based Services)	entropy	Location privacy protection called Safe Cycle Based Approach (SCBA)	Prorequest
Bin, Lei, & Guoyin (2019)	LBS	entropy	Ɛ -sensitive correlation privacy protection	Prorequest
Sun, Chen, Hu, Qian, & Hassan (2017)	LBS	entropy	Entropy is used to devise methods to defend two attacks to LBS.	Elsevier
Du, Cai, Zhang, Liu, & Jiang (2019)	LBS	Entropy is used to measure the degree of privacy preservation for an anonymous set.	Entropy is used is used to measure the uncertainty of recognizing the user’s location in a dummy location set.	Prorequest
Ukil, Bandyopadhyay, & Pal (2015)	Smart Energy Management Systems	Proposed a model called Dynamic Privacy Analyzer	The proposed dynamic privacy analyzer for smart meters uses estimation of privacy disclosure risk through analytical framework.	IEEE
Bugeja, Jacobsson, and Davidsson (2020)	Smart Home	Based on data sensitivity score	Based on data sensitivity score	ACM
Daubert, Wiesmaier, & Kikiras (2015)	Smart Home	Trust - Trust is used as a scalar metric and mapped to privacy, sensitivity,	A model to link information, privacy and trust.	IEEE

Research Authors	Category	Privacy Metric	Privacy Method	Publisher
		and personally identifiable information.		
Kennedy, Li, Wang, Liu, Wang, & Sun (2019)	Smart Home - speakers	Semantic distance	Accuracy and semantic distance are used	IEEE

Table 3: Research on IoT Privacy Metric

APPENDIX B
Figure 1

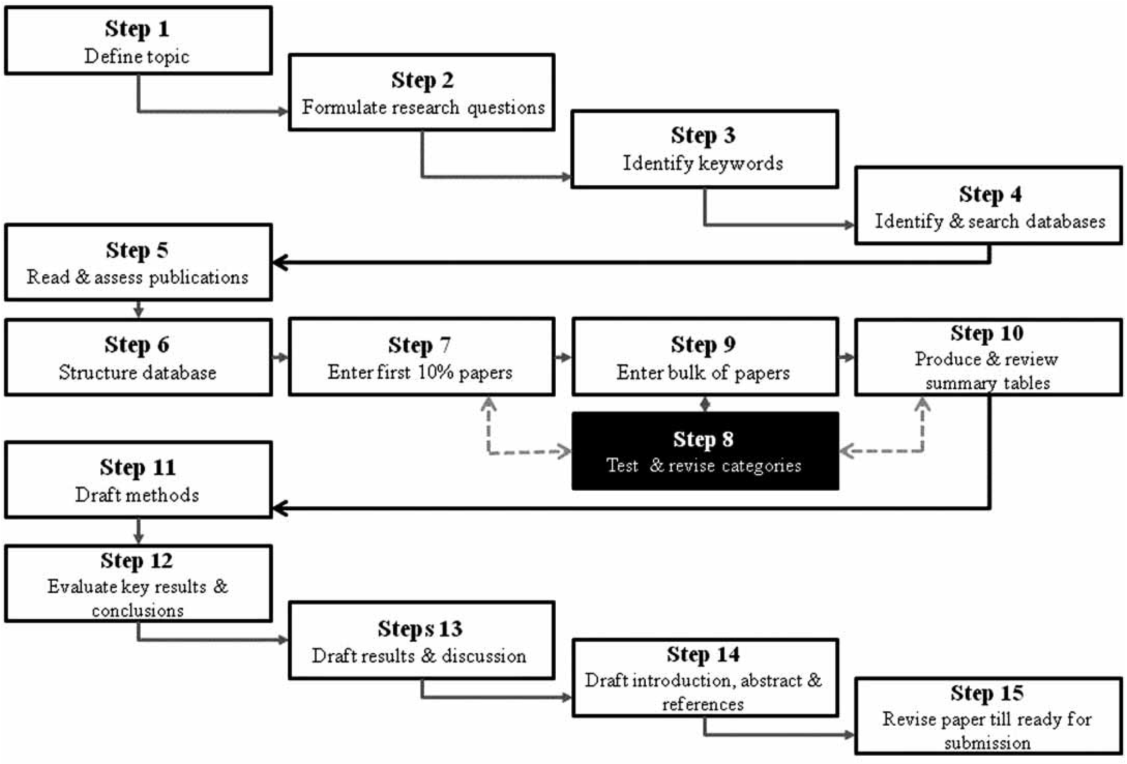

Step 1
Define topic
Step 2
Formulate research questions
Step 3
Identify keywords
Step 4
Identify & search databases
Step 5
Read & assess publications
Step 6
Structure database
Step 7
Enter first 10% papers
Step 9
Enter bulk of papers
Step 10
Produce & review summary tables
Step 8
Test & revise categories
Step 11
Draft methods
Step 12
Evaluate key results & conclusions
Steps 13
Draft results & discussion
Step 14
Draft introduction, abstract & references
Step 15
Revise paper till ready for submission

Figure 1: The fifteen stage literature review process by Pickering and Byrne (2014)

Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective

Kevin Slonka
kslonka@francis.edu
Computer Science & Cyber Security Department
Saint Francis University
Loretto, PA 15940 USA

Sushma Mishra
mishra@rmu.edu

Peter Draus
draus@rmu.edu

Natalya Bromall
bromall@rmu.edu

Computer and Information Systems Department
Robert Morris University
Moon Township, PA 15108 USA

Abstract

The constantly increasing number of security incidents and threats warrant organizational security governance (OSG) practices rooted in data that allow quick and reliable decision-making to quickly adapt to the changing landscape of security management. Measurement, reporting, and monitoring of security controls across organizations provide a data-driven governance approach that enables leaders to scale security tools and measures aligned to organizational business objectives. This research identifies standard practices under measurement, reporting, and monitoring and provides insight into how these domains come together to enhance overall OSG practices. Interviews are conducted with security professionals in multiple organizations. Qualitative analysis of the data suggests underlying themes for each domain. Results indicate that the three domains under study form the basis of data governance and play a key role in aligning the OSG objectives with security controls. Implications for research and practice are drawn, and future research directions are suggested.

Keywords: organizational security governance, data governance, measurement, reporting, monitoring, qualitative, thematic analysis

1. INTRODUCTION

Security measurement, reporting, and monitoring are critical components in all organizational security governance (OSG) strategies. Implementation of constant security monitoring enhances employees' security assurance behavior and awareness (Ahmad et al., 2019). Effective security measurement in all fields of the organizational IT infrastructure leads to effective information security management (You, Cho, & Lee, 2015). Finally, a successful reporting strategy is a glue that holds together all other areas of information security governance. With the increased number of cyber-attacks, top organizational management becomes more and more involved in security governance and requires constant reporting on (1) what was done to reduce vulnerabilities and (2) how effective these measures are (Garigue & Stefaniu, 2003). At the same time, even the involvement of top management does not guarantee effective prevention of cyber-attacks. Corris (2010) noted that organizations continue to fall victim to phishing, stolen data, employee negligence, and other security issues. While there is a solid OSG theoretical framework, few studies report the match between this framework and its practical implementation.

Researching the way organizations implement OSG measures will have multiple benefits. First, it will help close the gap between theoretical frameworks and the real issues organizations face with their implementation. Second, it will reveal the aspects of OSG that companies encounter the most difficulties. For example, previous research shows that OSG implementation is often inefficient due to either not formulating its specific objectives or not communicating them to all involved parties (Mishra, 2015). Finally, it will help the researchers provide recommendations for making OSG implementation more effective.

In this research, we use the theoretical framework of OSG defined by AlGhamdi (2020). This model includes seven critical domains (1) Responsibility & accountability, (2) Awareness, (3) Compliance, (4) Assessment & auditing, (5) Measurement, (6) Reporting, and (7) Monitoring. The research goal is to explore the practical implementation of the last three domains: organizations' measurement, reporting, and monitoring. The research goal yields three research questions, which will be answered in this study:
RQ1: How does security measurement structure influence Organizational Security Governance (OSG) practices?

RQ2: How do reporting initiatives influence OSG practices?

RQ3: How does monitoring influence organizations’ OSG practices?

2. LITERATURE REVIEW

Organizational Security Governance

Organizational Security Governance is part of the overall organizational Governance. Blum (2020) lists the main functions as “Charter or mandate the security program,” “Manage, control, and report on risk,” Coordinate security projects and manage issues,” Manage security policy,” and “Allocate security budgets and resources.” It is essential to recognize that this is a governance activity and not simply a framework for IT security. Schinagl, S., & Shahim, A. (2020) noted the move from the technical level to the top board, strategic level when they wrote, “landscape has shifted ‘from the basement to the boardroom,’ that is, from a narrowly focused technical issue towards a strategic business issue and a top priority item for the board” (Schinagl & Shahim, 2020, p. 283).

Another driving force behind the expansion into the boardroom is the increasing number of laws and regulations impacting data, privacy, and security. Khoo, Harris, & Hartman (2010) wrote, “Organizations must elevate the issue to a corporate governance priority to systematically strengthen information security at all levels of the organization” (p. 51). Yaokumah & Brown (2014) looked at the relationship between strategic information security governance and information security governance and concluded that “effective information security governance strategic alignment greatly improves organizations’ risk management, resource management, performance measurement, and delivers business value” (Yaokumah & Brown, 2014 p. 51).

Frameworks

As the importance to the organization of the information and information infrastructure grew, and the governance structures expanded, some form of the system was needed to help organize the growing complexity. Multiple frameworks were utilized in this endeavor; some were part of the general organizational governance structure, and some were specific to the information security realm. Some of the frameworks, such as ISO/IEC 38500 and COSO, have high levels of abstraction and are focused more on governance itself, while others, such as ISO/IEC 17779 and ITIL, are focused more on IT tactics and strategy. Of course, this framework's more detailed and focused nature makes it more prevalent among technical managers and not overall organizational governance (Von Solms, 2005). Other frameworks cover higher governance levels down to the tactical level and are in the middle of the abstraction layer, such as COBIT 4/5 (De Haes, Van Grembergen, & Debreceny, 2013). Al-Fatlawi (2021) looked at using COBIT 5 to improve security in accounting information systems and noted that the framework included the governance and implementation processes.

While COBIT is a prevalent and successful framework, other researchers have found deficiencies in its use for information security (Pratiwi, Indah, Jauhari, & Firdaus, 2020). AlGhamadi (2020) reviewed the literature in this area and found seven critical success factors when using frameworks for information security governance: 1) Responsibility & Accountability, 2) Awareness, 3) Compliance, 4) Assessment & Auditing, 5) Measurement, 6) Reporting, and 7) Monitoring.

Problems with the Current Situation

Some of the problems with the current situation in Information Security Governance include the lack of oversight by top organization leaders. One group of researchers, after reviewing security governance in the healthcare industry, concluded that the increasingly complex laws and regulatory environment exasperated the problems, writing, "The preponderance of healthcare-related laws, compliance regulations, and security guidance frameworks serve to complicate the cybersecurity challenge further and too often results in senior leadership assuming a state of blissful ignorance" (Abraham, Chatterjee, & Sims, 2019, p.539).

In addition to the breadth of the framework, others have noted the difficulty in measurement and reporting. To try and help solve this problem, some researchers have focused on developing methodologies to assist the security assessors in their duties. They found that the data was "deeply influenced by the expertise of the assessor and his/her sensitivity" (Angelini, Bonomi, Ciccotelli, & Palma, 2020, p. 1). The complexity of the entire process and the disconnect from the everyday work of most employees was also listed as an issue by Ridley, Young, and Carroll (2004). Sadok, Alter, & Bednar (2020) conclude that "Security practices remain an illusory activity in their real-world contexts" (p. 18).

Measurement & Monitoring

When gathering data for security evaluation, it still isn't clear what the measurement should be. Lidster & Rahman (2018) performed a comprehensive literature review and concluded a lack of a good measure of alignment between practices and governance still exists. It is not just governance that can be improved by including the upper level of the organization. A group of researchers found that the quality of the security is enhanced as the quality of the relationship between the auditors and upper management improved (Steinbart, Raschke, Gal, & Dilla, 2018).

One area where adherence to governance policies is the area of phishing attacks. Testing and data gathering in this area is easy and done across many organizations. Instead of looking at actual testing, some researchers have suggested gathering data on the user's knowledge of phishing and their understanding of different situations using scenario-based analysis. In this way, they hope to collect data on the employees' broader understanding of the issues and opportunities for data loss (Das, Nippert-Eng, & Camp, 2022).

As with so many other aspects of the information arena, the collected data must be stored, sorted, and ready for analysis. For security issues, reports of flaws are stored in multiple open databases, such as the Common Vulnerabilities and Exposures (CVE) and National Vulnerability Database (NVD). Security policies developed from the governance models can refer to these vulnerabilities when ensuring that systems securities are up to date. Dong et al. (2019) found inconsistencies in the data between these two repositories, making auditing difficult.

As the information infrastructure grows and data is no longer stored in central locations but on devices scattered all over, such as in an IoT environment, security and measurement become an even more significant hurdle. IoT devices are built by smaller companies, each with data and security standards. They lack the resources to match standards for every customer. The expanded usage of such devices outstrips the regulatory and governance as demand pressure increases (Vitunskaite, He, Brandstetter, & Janicke, 2019).

The issue is more than the framework but the organization's security practices. Orehek and Petric (2020) stress that the goal of measurement should not just be on individual metrics but that all the data should be evaluated to measure the organization's security practices. Others have noted that by extending the security practices, workers are working to meet specific security metrics and improve the entire organizational security levels (Tan, Ruighaver, & Ahmad, 2010, September), leading to reporting such overall levels.

Reporting

One of the most basic IT security reports is a security audit. While the audit may or may not look at the governance model, it still collects data on security policies and adherence. Bongiovanni et al. (2022) argue that the problem is not in the data gathering but in quantifying and organizing the data to align with the organizational governance model. They proposed a model to quantify existing security data to an existing security governance model. They tested their model on multiple organizations and confirmed that such a model worked as proposed and tracked well across industries. Instead of developing a new reporting model, Herath, Herath, & Cullum (2022) proposed using the Balanced Scorecard model and applying it to security governance. One of the advantages of this method is that all of the previous work could be leveraged in the deploy reporting scheme. Another positive is the inclusion of the financial return on the investment in security governance that is inherent in this model.

Alotaibi, Furnell, & Clarke (2019) proposed a reporting model that assigns points to end-users based on their security compliance and awareness of security policies and risks. The intriguing aspect of this model is that the issues are not just used as a measurement and reporting function but are used to assign both penalties and rewards.

One of the significant areas of reporting is a risk. Spremic (2011) pointed out that IT risk is a function of both the asset itself and the threat and vulnerability. Three parts of the proposed corporate IT risk management model are: "Corporate governance policies for managing IT risks," "Procedures for managing IT risks on business units level or functional level," and "Operational (technical) activities."

Organizational Security Governance Practices

As demonstrated earlier, changing the practices to increase the upper levels of management in the security governance improves security levels. Still, other researchers have found more of a sense of complacency. After interviewing 187 employees in 39 organizations about their security practices, Sadok, Alter, & Bednar (2020) found that the corporate policies were disconnected from the security activities of the workers and that the security policies don't have a high priority. They concluded that "Security practices remain an illusory activity in their real-world contexts." Sadok, Alter, & Bednar (2020 p.1). The organization's security practices are more than the policies and governance structure; it is also how the employees interact with the guidelines. What is said and rewarded in all organizations is not always the same. Khatib & Barki (2021) surveyed over 300 workers concerning their activities in hypothetical scenarios and found their response was motivated more by any benefits than any costs based on non-compliance. This would fit with the model proposed by Alotaibi, Furnell, & Clarke (2019).

Efficient OSG practices are not just an organization's security policies but encompass the training and everyday interactions with the guidelines; some of those interactions increase the security level, and some decrease the organization's security level (Da Veiga et al., 2020). Other researchers have moved beyond security practices and looked at the interplay between security practices and the general practices of the organization and information security awareness. They found a high correlation between the general practices and the security practices, suggesting that training efforts on security practices alone should be a more effective use of resources (Wiley, McCormac, & Calic, 2020). Of course, the security practices depend on a top to bottom security governance framework. After reviewing industry and academic security practices, Veiga & Eloff (2007) made the critical recommendation that "The first step in developing an information security culture and empowering the workforce to be aware of their responsibilities towards protecting information assets would be to implement a comprehensive Information Security Governance framework" (p. 370).

To fully understand an organization's Information Security Governance, we need to gather data about the structure and policies and conduct interviews concerning all aspects of the organization's security practices.

3. METHODOLOGY

Data Collection and Analysis

To collect the data, we conducted 10 interviews with security and organizational governance managers, which were sufficient to cover small, medium, and large businesses. The discussions included questions about the managers' experience with security measurement, reporting, and monitoring. Each interview included three groups of questions matching the three domains. Each question included multiple talking points (Table 1), which were normally covered by the respondents. In case any talking points were skipped, the interviewer asked additional questions related to the missing information.

Question 5: How does measurement influence OSG practices?
• How does your organization measure its performance against their Organizational Security Objectives? ○ Can you give some examples of the types of data that is gathered to help measure this performance? ○ IS the data actually used to try and alter performance? ○ Does the data only flow upward, or do all employees have access to at least some of these performance measures? ○ Do you have any examples of this downward flow?
• In what ways are employees measured on their awareness and commitment to the Organizational Security Objectives? ○ Is the measurement itself meant to influence their performance? ○ Can you give any details?
• Does your organization gather data from outside to assess their Organizational Security Objectives? ○ Can you give some details? ○ Does this data influence practice as well as data gathering techniques and measures?

Table 1: Interview Questions Structure

The interviews were recorded as audio files and later converted to text with the help of a transcribing tool. The answers were grouped by the three domains and the respondents within each domain. During the first stage of the further analysis, we listed the themes that emerged after the initial reading. A theme was recorded on the list if it was mentioned multiple times, either by the same respondent or multiple respondents. The responses were specifically matched to the recorded themes during the second stage.

The results of the data analysis are presented in the following section.

The subjects' demographic information is given in Appendix A. The majority of the ten interviewed subjects represent either the top management or executive management highly involved in information security decision-making. Most respondents represent medium to large organizations (1000 or more employees) and have substantial (10 or more years) experience in their field. The organizations were very diverse and included healthcare, pharma, defense, financial services, engineering/IT, and non-profit.

4. RESULTS

This section presents the results of our data analysis. The data is presented research question-wise.

Domain: Measurement

Theme 1: Performance	• Dashboard with metrics for each area • Different areas of performance: people, process, and knowledge • Delivery of completed projects • Projects within budget • Frameworks provide metrics • Internal audit performs measurement. • Key risk indicators • KPIs are measured but do not get much of an executive view-operational nature, such as VM and phishing. • Good code passing through pipeline offering good service
Theme 2: Awareness of OSG	• Maintain situational awareness through different channels • Reputation awareness
Theme 3: External	• Third-party measures • Security campaigns impact • Training impact • Scans the internet-facing systems for threat vectors • Provide a score to reflect the health of the system • Ranks highest risk systems to prioritize • Sends assessment reports to clients directly

Table 2: Measurement Domain Themes

A well-designed OSG program needs to be constantly aligned with the organization's risk appetite. Measurement of governance practices in control effectiveness, risk score, policy effectiveness, and operational efficiency ensure that the OSG objectives are realized after implementation. Performance and changes in an organization must continually evaluate whether the OSG principles, policies, and procedures are working according to predefined indicators and criteria (Alghamdi et al., 2020). Research literature suggests many measures, such as employees' awareness and training in doing their job, clarity in business processes (Mishra, 2015), knowing who to approach in adverse situations, and commitment to responsibilities (Nicho, 2018). These measurements assure top management that the OSG program is on track and acts as an incentive to garner more resources for the enhancement of the program.

Our data for the Measurement domain shows three emergent themes: 1) Performance, 2) Awareness of OSG, and 3) External (Table 2).

Theme one covers the performance measurement indicators and practices. Our data suggest that most organizations use dashboards with metrics for each performance area. These areas are people, processes, and knowledge. Multiple types of metrics are used, such as the delivery of completed IT projects, the number of projects within budget, and key risk indicators, such as the number of phishing attacks, malware attacks, etc. The internal audit division performs measurements of control effectiveness in many organizations. Most of the leading IT governance frameworks provide key metrics. Key performance indicators (KPI) are measured, funneling data to dashboards. Operational KPIs include whether the code passing through the pipeline is good, whether managers use vulnerability management, or detecting phishing attacks. In contrast, dashboard data is provided to C-Level executives.

Theme two is about employees' awareness of OSG practices. Our data suggest that it is essential to maintain situational awareness through different channels in various contexts. Understanding what is being measured, why it is being measured, and how it impacts day-to-day tasks goes a long way in making measurement more effective. Employees' reputation awareness creates a sense of pride in their daily work performance.

Theme three is about using external factors and agencies to measure OSG practices' impact. Several third-party measures are used in organizations. Third parties are often used to track the impact of security campaigns or training employees. On the network side, scanning the internet-facing systems for threat vectors allows for measuring network efficiency. On the process side, frameworks entail guidelines that will enable creating a score on processes to reflect the system's health. The prioritized ranking for different controls allows for better decision-making. For DoD-related organizations, external agencies directly send the report of OSG practices to the clients to maintain transparency in the process.

Domain: Reporting

Reporting allows the actual data from measurement to flow upwards in the organization such that decision-making is informed and timely. Reports show the results of the assessment and measurement activities in the organization, which can assist top management in understanding the return on investment in the organization's protection (Alghamdi et al., 2020). Research literature argues for proper reporting channels in the context of OSG to achieve the intended benefits of the controls (Mishra, 2020; Nicho, 2018). Most widely used frameworks such as COBIT, NIST, or even in-house versions of such frameworks provide a rich array of metrics for reporting purposes.

Our results suggest three main themes for the reporting domain: 1) Standard procedure, 2) operations, and 3) action related to reports (Table 3).

Theme one is reporting on standard procedures at different levels of an organization. Our data suggest that monthly operational reporting is funneled up through metrics and KPIs to management. Teams of people create reports through Tableau (or similar tools) for CEOs for strategic decision-making. Once a month, data is reported at a C-level meeting without daily operational details. Quarterly reports with crucial metrics for the board are also generated. In larger organizations, there are separate reporting groups specializing in reporting on anything that occurs in the organization; for example, risk assessment reports based on the state of controls are generated for auditors. In some organizations, reporting depends on who is asking and what is being asked; it is in response to what is being sought. There are no standardized formats for enterprise-wide reporting. Rather, departments have their standards of reporting. Some organizations follow reporting standards provided by frameworks such as US-CERT.

Theme two is operational reporting for task management activities at a higher granularity. Our data suggests that organizations use multiple tools to obtain any kind of report aligned to security process and control. It could be vulnerability reports from the third party or real-time information on all domains of cybersecurity that are essential for daily tasks to be completed. Measuring all the controls in multiple manners allows consistent control appraisal in a given control domain.

Theme three alludes to actions taken in response to these reports. The organizational focus is to refine and improve the OSG process through reports and metrics. The flow of information upwards and downwards through the hierarchy depends on the information's value or nature and urgency. High-risk situations are acted upon in real-time. Compliance with policies is an expectation, followed up diligently in reporting. Non-compliance with controls or unexpected conditions, such as a breach, warrants more training for staff to deal with the situation. There could be a reward system to encourage employees to do the right things. It is good to recognize employees for due diligence in reporting incidents or unexpected situations.

Domain: Monitoring

Continuous monitoring provides agility to an organization's response to an aberration in its systems or processes. Monitoring allows responding to situations if preventive controls have been bypassed deftly. Monitoring control allows for quick remediation of the problem and minimizes damage in an unwarranted case (Mishra, 2021). Monitoring provides business continuity and recovery plans to be executed without interrupting day-to-day business (Alghamdi, 2020). Monitoring also allows for oversight of the users' behavioral patterns within the organization to ensure that data is confidential and integrity is maintained (Mishra, 2015).

Our data suggest three themes in the domain of monitoring: 1) continuous monitoring, 2) action in deviation situations, and 3) monitoring training (Table 4).

Theme one is about continuously monitoring the IT environment using multiple tools. Organizations implement zero-trust security, which results in everything and everyone being monitored on the network. Tools are used to scan many terabytes of data daily. Baseline parameters are configured, and the dashboard captures the anomalies that need attention. Automated recurrent monitoring allows for ensuring that controls are operating effectively. All monitoring data feeds into reports directly for compliance purposes.

Theme 1: Standard procedure	• Monthly operational reporting funneled up through metrics and KPIs to management. • Reporting depends on who is asking and what is being asked. • Not standardized. Departments have their standards of reporting. • Team of people creating reports through Tableau for CEOs • Reports quarterly with crucial metrics for the board • Once a month, data is reported at a C-level meeting. • A separate group presents a technical report on anything important that is ongoing. • Risk assessment reports based on the state of controls • Follow US-CERT reporting standards.
Theme 2: Operations	• Tools allow obtaining any kind of report aligned to security process and control. • Vulnerability reports from the third party • Real-time reports on all domains of cybersecurity • Constant Control appraisal in a given control domain
Theme 3: Action related to reports	• The focus is to refine and improve the process through reports and metrics • Depends on the value of the information. High-risk situations are acted upon in real-time. • Compliance is an expectation. Follow it diligently • Non-compliance or unexpected situations warrant more training. • Recognize employees for due diligence in reporting incidents or unexpected situations

Table 3: Reporting Domain Themes

There are structures in place, such as a change advisory board, that allow what is monitored and how the data is being consumed for decision making.

Theme 1: Continuous monitoring	• Continuously monitoring our environment. • Zero trust security-everything and everyone is monitored. • All data feeds into reports for compliance. • Change advisory board allows what is monitored. • Tools are used to scan many terabytes of data daily. • Automated recurrent monitoring to ensure controls are operating effectively
Theme 2: Action in deviation situations	• Employees know what to do. • In deviation, act according to policies. • Sensitive information is flagged and put in the proxy area. • Human intervention is required to clear the doubt. • Advisory decides actions based on the situation. • Something gets flagged, then a report is sent to everyone
Theme 3: Monitoring training	• What to do in a deviation situation is a part of awareness training • Specific training is required to allow what changes can go through. • Vulnerable to phishing attacks-needs to be trained

Table 4: Monitoring Domain Themes

Theme two is about actions taken in an unexpected situation. Our data suggest that there is training so that employees know what to do in unexpected situations. If there is no clarity for a given scenario, then employees are trained to follow policies as guidelines. In many cases, human intervention is required to clear the ambiguity in action. Monitoring allows the organization to flag sensitive information traveling in the network and put it in a proxy area for further review. There are advisory groups in organizations that decide what actions are best based on the situation. In most cases, if something gets flagged, then an alert is sent to everyone.

Theme three is about specific training for monitoring purposes. Employees on monitoring teams need to be provided specialized training in a) recognizing that a situation is not normal and b) what should be the course of action in a situation like this. It could be a vulnerability or phishing training that provides detailed steps on what changes can be allowed and what cannot be done.

5. DISCUSSION

Each of the three domains (bolded in Table 5) in this study has implications for practice. The first domain, measurement, can be considered the gatekeeper to the remaining domains. Without proper measurement, there can be no reporting or monitoring. This study suggests that measurement must be implemented at various levels within an organization in order to be effective. At the operational level, software engineers need measurement of their code as it passes through the CI pipeline. Compliance staff needs measurement of security control implementation for audit purposes. At a higher level, managers use KPIs and KRI's to ensure that organizational goals are being met and risks are being mitigated. At the strategic level, completed projects and budgets must be measured to achieve proper prioritization. While organizations may need to develop certain metrics in-house, there are various external resources that offer frameworks containing sets of common measures that every organization should implement (Chew et al., 2008; Bodeau et al., 2018). Organizations, however, should ensure that they are not merely implementing measurement for its sake; "inappropriate levels of precision and stability" (Snyder et al., 2020, p. 42) increase for little to no gain. Only measurements that help achieve business goals should be implemented, monitored, and reported.

Performance Awareness of OSG External	**Measurement**
Standard procedure Operations Action related to reports	**Reporting**
Continuous monitoring Action in deviation situations Monitoring training	**Monitoring**

Table 5: Domain Theme Summary

Just as measurements, suggestions for proper reporting can be found in external frameworks. Organizations will find that these are merely suggestions and will be highly customized depending on the recipient. C-Suite executives may want reports that are infrequent and high-level, while middle managers may want reports that are frequent and detailed. Some reporting may even be conducted in real-time, such as critical vulnerability reports from the cyber team. The same rule applies with reporting as it did with measuring, don't go overboard. Over-reporting can lead to report fatigue, leading to critical reports being glossed over or deleted without being read. This can have catastrophic effects on a business.

Newer cyber frameworks have given birth to the younger brother of reporting: continuous monitoring. While reports offer insights into an organization's operations on a periodic basis, critical activities can occur between those periods. Organizations must implement tools and processes to ensure that their environment is monitored 24/7 for changes to baseline performance (National Institute of Standards and Technology, 2018). This can be everything from increasing processor and memory usage on a production database server to detecting changes to a configuration file on a domain controller. Unwanted change on a network can wreak havoc, and employees must be properly trained to respond to such incidents. The existence of an incident handling team to respond to cyber breaches is one such way an organization can prepare for negative changes (Cichonski et al., 2012). In a more proactive sense, an organization should have a configuration control board (CCB) to approve or deny any change to the network, ensuring that proper testing is done and the change will not negatively affect the organization's security posture (Johnson et al., 2011).

6. CONCLUSION

This study makes abundantly clear that proper OSG is mandatory for organizations to succeed in today's threat landscape. Key aspects of measuring, reporting, and monitoring were uncovered and the existence and usefulness of these three domains were validated. Given the sheer quantity of effort required to implement these three domains alone, it is evident that proper OSG cannot be achieved with fractional IT staff nor with one- or two-person IT departments. It takes a team (optimistically many teams) of adequately educated and trained cyber experts to ensure a resilient security posture and protect an organization from ever-changing threats. Future research should be conducted that takes results from all seven domains from the seminal study and produces a set of minimum guidelines for implementing of an OSG program within an organization.

7. REFERENCES

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business Horizons*, *62*(4), 539-548.

Ahmad, Z., Thian, S. O., Tze, H. L., & Norhashim, M. (2019). Security monitoring and information security assurance behavior among employees: An empirical analysis. *Information and Computer Security, 27*(2), 165-188.

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and it governance under cobit 5 framework: A case study. *Webology, 18* (Special Issue on Information Retrieval and Web Search), 294-310.

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security, 99*, 1-39.

Alotaibi, M. J., Furnell, S., & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information & Computer Security, 27*(1),2-25.

Angelini, M., Bonomi, S., Ciccotelli, C., & Palma, A. (2020). *Toward a Context-Aware Methodology for Information Security Governance Assessment Validation*. International Workshop on Cyber-Physical Security for Critical Infrastructures Protection, Springer, 171-187.

Bodeau, D. J., Graubart, R. D., McQuaid, R. M., & Woodil, J. (2018). *Cyber resiliency metrics, measures of effectiveness, and scoring*. MITRE Corporation. https://www.mitre.org/sites/default/files/publications/pr-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf

Bongiovanni, I., Renaud, K., Brydon, H., Blignaut, R., & Cavallo, A. (2022). A quantification mechanism for assessing adherence to information security governance guidelines. *Information & Computer Security.*

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Corris, L. (2010). *Information security governance: Integrating security into the organizational culture*. Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, 35-41.

Das, S., Nippert-Eng, C., & Camp, L. J. (2022). Evaluating user susceptibility to phishing attacks. *Information & Computer Security, 30*(1), 1-18.

Da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 1-23.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems, 27*(1), 307-324.

Dong, Y., Guo, W., Chen, Y., Xing, X., Zhang, Y., & Wang, G. (2019). *Towards the detection of inconsistencies in public security vulnerability reports*. 28th USENIX Security Symposium (USENIX Security 19), 869-885.

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security, 12*(4), 36-40.

Herath, T. C., Herath, H. S., & Cullum, D. (2022). An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks. *Information Systems Frontiers*, 1-41.

Johnson, A., Dempsey, K., Ross, R., Gupta, S., & Bailey, D. (2011). *Guide for security-focused configuration management of information systems*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

Khatib, R., & Barki, H. (2021). How different rewards tend to influence employee non-compliance with information security policies. Information & Computer Security, 30(1), 97-116.

Khoo, B., Harris, P., & Hartman, S. (2010). Information security governance of enterprise information systems: An approach to legislative compliant. *International Journal of Management & Information Systems (IJMIS), 14*(3).

Lidster, W. W., & Rahman, S. S. (2018, August). *Obstacles to implementation of information security governance.* 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 1826-1831.

Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security, 23*(2), 122-144.

Mishra, S. (2020). Examining Organizational Security Governance (OSG) Objectives: How strategic planning for Security is undertaken at ABC Corporation? *Journal of Information Systems Applied Research, 13*(2), 13-24.

Mishra, S. (2021). Interpreting Organizational Security Governance Objectives for Strategic Security Planning, *Journal of Information Systems Applied Research, 14*(3), 30-43.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Nicho M. A process model for implementing information systems security governance. *Information & Computer Security. 2018, 26*(1), 10–38.

Orehek, Š., & Petrič, G. (2020). A systematic review of scales for measuring information security culture. *Information & Computer Security, 29*(1), 133-158.

Pratiwi, A., Indah, D. R., Jauhari, J., & Firdaus, M. A. (2020, May). *Security capability assessment on network monitoring information system using COBIT 5 for* *information security.* In Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019), 167-171.

Ridley, G., Young, J., & Carroll, P. (2004, January). *COBIT and its Utilization: A framework from the literature*. In 37th Annual Hawaii International Conference on System Sciences, 1-8.

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: exploring the disconnect between corporate security policies and actual security practices in SMEs. *Information & Computer Security, 28*(3), 467-483.

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance?"From the basement to the boardroom": towards digital security governance. *Information & Computer Security, 28*(2), 261-292.

Snyder, D., Mayer, L. A., Weichenberg, G., Tarraf, D. C., Fox, B., Hura, M., Genc, S., & Welburn, J. W. (2020). *Measuring cybersecurity and cyber resiliency*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2703/RAND_RR2703.pdf

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both?. *Computers & Security, 24*(2), 99-104.

Spremic, M. (2011, July). *Standards and frameworks for information system security auditing and assurance.* In Proceedings of the World Congress on Engineering, 1, 251-266.

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29.

Tan, T. C., Ruighaver, A. B., & Ahmad, A. (2010, September). Information security governance: When compliance becomes more important than security. In IFIP International Information Security Conference (pp. 55-67). Springer, Berlin, Heidelberg.

Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information systems management, 24*(4), 361-372.

Vitunskaite, M., He, Y., Brandstetter, T., & Janicke, H. (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security, 83*, 313-331.

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security, 88*, 1-8.

Yaokumah, W., & Brown, S. (2014). An empirical examination of the relationship between information security/business strategic alignment and information security governance domain areas. *Journal of Law and Governance, 9*(2), 50-65.

You, Y., Cho, I., & Lee, K. (2015). An advanced approach to security measurement system. *The Journal of Supercomputing, 72*(9), 3443-3454.

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security, 28*(5), 681-700.

Editor's Note:

This paper was selected for inclusion in the journal as the CONISAR 2022 Best Paper The acceptance rate is typically 2% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.

APPENDIX A
Participants – Demographics

Participants	Relevant years of experience	Industry	Size	Title	Education level
P1	10+	Pharma	40,000+	Information Security Manager	Master
P2	10+	Financial services	1000+	Cyber Risk advisory manager	Doctoral
P3	6+	Financial services	10,000+	Senior cyber security investigative analyst	Master
P4	20+	Healthcare services	10,000+	VP security	Master
P5	3-5	Engineering/IT	80	Studio lead	Bachelors
P6	15	Non-profit R&D (fed contractor)	65	President/CEO	Doctoral
P7	7	Financial services	200,000+	VP cyber security operations	Masters
P8	23	Defense/ aerospace	400	CISO & CIO	Bachelors
P9	9+	Technology consulting	Global/big	Global Director Security Architecture and Governance and Cloud Security and Compliance Services for Digital Solutions	Bachelors
P10	25	Healthcare	90,000+	Information Security Manager	Master

CyberEducation-by-Design

Paul Wagner
paulewagner@arizona.edu
Department Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona

Abstract

Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million to 3.5 million for 2021 and the United States' estimates range from 465,000 to over 700,000 open jobs as of September 2022. The most optimistic estimates still demonstrate a critical issue. Many approaches to this problem take a siloed approach of improving or introducing cybersecurity curriculum at a younger age, focus on point in time training and certification, or skills development through internships, apprenticeships, and work experience. Solving this problem requires an integrated approach that incorporates education, training and certification, and experience that is accessible to all, at any age or experience level. This paper will propose a CyberEducation-by-Design methodology and framework. This methodology and framework is based on a review of current government initiatives and legislation that recognizes and addresses the cybersecurity education and workforce development problem. Additionally, standards and curriculum available for K-12, Community and 2-Year Colleges, and 4-Year and beyond institutions will be outlined to cover the educational aspects of the problem. Further, skills development through certifications, On-the-Job-Training (OJT) and internships / apprenticeships, experiential learning, and work experience will be discussed.

Keywords: Cybersecurity Education, K-12 Education, Workforce Development, Certification

1. INTRODUCTION

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy (Biden, 2021). This is evidenced by the recent Colonial Pipeline Attack (Turton, 2021); SolarWinds Attack (CIS, 2021); and ransomware attacks against healthcare systems (Weiner, 2021), U.S. schools and colleges (Kshertri, 2021) and critical infrastructure (Cluley, 2021). Most survey results agree that there is a current and ongoing shortage of skilled cybersecurity workers that places our privacy, infrastructure, and nation at risk. Estimates for the global Cybersecurity Workforce Gap range from 2.72 million (ISC2, 2021) to 3.5 million (Cyber Academy, 2021) for 2021 and the United States' estimates range from 465,000 (Brooks, 2021) to over 700,000 (Cyber Seek, 2022) open jobs as of November 2021. The most optimistic estimates still demonstrate a critical issue. Many approaches to this problem take a siloed approach of improving or introducing cybersecurity curriculum at a younger age, focus on point in time training and certification, or skills development through internships / apprenticeships, and work experience. The purpose of this paper is to propose a CyberEducation-by-Design Framework. This framework takes elements from various siloed initiatives to consolidate approaches that incorporates education, training and certification, and experience that is accessible to all at any age or experience level. Supporting this framework is a review of current government initiatives and legislation that recognizes and addresses the cybersecurity education and workforce development problem. Additionally, standards and curriculum available for K-12, Community and 2-Year Colleges, and 4-Year and beyond institutions will be outlined to cover the educational aspects of the problem. Further, skills development through certifications, On-the-Job-Training (OJT) and internships / apprenticeships, experiential learning, and work experience will be discussed.

2. PROPOSED WORK

Research Design and Methodology

The author used a systematic literature review (SLR) technique to find relevant academic articles from 2010 to 2021. Relevant information was extracted from select articles to inform analysis and discussion. The steps involved in the SLR process include:

1. Define the research questions.
2. Determine the data sources and search process.
3. Inclusion and Exclusion Criteria.
4. Results of searching and data extraction.
5. Analysis and Discussion.

Research Questions

1. What U.S. government legislation or initiatives have been developed to address cybersecurity education and workforce development?
2. What standards, curriculum, and initiatives have been introduced to address the cybersecurity and workforce development issues facing the U.S.?
3. What can be done to address the cybersecurity and workforce development issues or improve upon current efforts?

Data Sources and Search Process

A variety of sources were used to identify relevant sources for this research including Google Scholar, IEEE, Elsevier, EBSCO, Proquest and other library resources. Additionally, current industry trend reports were analyzed to identify current and relevant statistics to support research objectives. Search terms included but were not limited to linking the term "Cybersecurity" to Education, K-12 Education, Legislation, Dual Enrollment, Certifications, and Safety. The search limited results from 2010 to present.

Inclusion and Exclusion Criteria

Given the limited, specific research on K-12 Cybersecurity education and its application to current cybersecurity workforce shortages, the author applied a liberal inclusive set of search criteria. Full-text journal articles were used to identify and analyze the current initiatives in cybersecurity education and training and current issues with cybersecurity workforce development. Information from these articles were extrapolated for their potential use in developing the CyberEducation-by-Design framework. Editorials, trade journals, and other online resources were used to identify the latest statistics, applications, and concerns facing cybersecurity education and workforce development.

Search Results

Search results can be broadly categorized into cyber-safety, cyber-education, and cyber-skills. The table provided in Appendix A focuses on the efforts to address the cyber education and workforce development issues; however, supplemental and supporting references are provided in the reference section.

3. GOVERNMENT LEGISLATION

Arguably, "Cybercrime" and the need for cybersecurity professionals has been around for nearly two centuries when a pair of thieves hacked the French Telegraph System to steal financial market information in 1834 (Herjavec, 2019). Since that time, cybercrime and cyber warfare has become more commonplace and sophisticated. Despite this long need for cybersecurity professionals, it wasn't until President Reagan signed into law the Computer Security Act of 1987 directing the National Bureau of Standards to, "establish a computer standards program for Federal computer systems, including guidelines for security of such systems drawing on technical security guidelines developed by the National Security Agency (NSA)." (Glickman, 1988, p. 6). President Clinton established the President's Commission on Critical Infrastructure Protection in 1996 and released the first national strategy for protecting the nation's computer networks from attack in 2000 (Clinton, 2000).

In 2003, President Bush released The National Security Strategy to Secure Cyberspace which articulated five national priorities:

I. A National Cyberspace Security Response System,
II. A National Cyberspace Security Threat and Vulnerability Reduction Program,
III. A National Cyberspace Security Awareness and Training Program,
IV. Securing Governments' Cyberspace, and
V. National Security and International Cyberspace Security Cooperation (Bush, 2003).

Four major actions and initiatives tied to Priority III which directly relates to this paper include:

- Promote a comprehensive national awareness program to empower all Americans; businesses, the general workforce, and the general population, to secure their own parts of cyberspace,
- Foster adequate training and education programs to support the Nation's cybersecurity needs,
- Increase the efficiency of existing general cybersecurity training programs, and
- Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications (Bush, 2003).

President Obama led many initiatives to improve the nation's cybersecurity. Briefly, these include the Cyberspace Policy Review (2009), making U.S. Cyber Command permanent (2009) (Armerding, 2013), issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity (2013)," which led to the National Institute of Standards and Technology (NIST) developing the Cybersecurity Framework (2014) (Obama, 2013), development of the Cybersecurity Act which includes Cybersecurity Information Sharing, National Cybersecurity Advancement, Federal Cybersecurity Workforce Assessment, and a variety of other cyber matters (2015) (Obama, 2015), and the implementation of the Cybersecurity National Action Plan (CNAP) which established the Commission on Enhancing Cybersecurity, modernize government IT, empower Americans to secure their online accounts (CNAP, 2017). CNAP enhanced cybersecurity education and training, through the National Initiatives for Cybersecurity Education (NICE) to expand Scholarship for Service opportunities, develop a cybersecurity core curriculum, and strengthen the National Centers for Academic Excellence in Cybersecurity Program.

President Trump issued Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which focused on modernizing federal information technology infrastructure, working with state and local government and private sector partners to more fully secure critical infrastructure, and collaborating with foreign allies (CISA, 2020). In response to this, The Department of Commerce and Department of Homeland Security investigated cybersecurity workforce development determining the following:

- The U.S. cybersecurity workforce needs immediate and sustained improvements,
- It is necessary to expand the pool of cybersecurity candidates through retraining and by increasing the participation of women, minorities, and veterans,
- There is a shortage of cybersecurity teachers at the primary and secondary levels, faculty in higher education, and training instructors, and
- Comprehensive and reliable data about cybersecurity workforce positions needs and education and training programs are lacking (CISA, 2020).

Most recently, President Biden issued his Executive Order to improve U.S. cybersecurity which focuses on removing barriers to threat information sharing between government and the private sector, improve software supply chain security, establish a cybersecurity safety review board, create a standard playbook for responding to cyber incidents, improve detection of cybersecurity incidents on federal government networks, and improve investigative and remediation capabilities (Biden, 2021). Additionally, the K-12 Cybersecurity Act of 2021 was signed into law ordering CISA to conduct an analysis of how cybersecurity risks specifically impact K-12 educational institutions, conduct an evaluation of the challenges K-12 educational institutions face in securing information systems and student records and implementing cybersecurity protocols, identifying cybersecurity challenges relating to remote learning, and evaluate the most accessible ways to communicate cybersecurity recommendations and tools (Cybersecurity Act, 2021).

4. STANDARDS ORGANIZATIONS

Several standards organizations are involved in overcoming the cybersecurity workforce gap in response to or in support of these government initiatives. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-181, Workforce Framework for Cybersecurity (National Initiatives for Cybersecurity Education (NICE) Framework), provides a set of building blocks for describing the tasks, knowledge, and skills (TKS) that are needed to perform cybersecurity work performed by individuals and teams for employers, education and training providers, and learners (Petersen, 2021). The NICE Framework attempts to define the TKSs in generic terms that can be applied to all organizations and are agile, flexible, interoperable, and modular (Petersen, 2021). The NICE Framework is comprised of seven categories of common cybersecurity functions which are broken down into 33 specialized areas that have defined Knowledge, Skills, and Abilities (KSAs) to complete defined tasks for that specialized area.

Additionally, Capability Indicators for Entry, Intermediate, and Advanced roles across training, experiential learning, education, continuous learning, and credentials / certifications are defined. These items provide the building blocks for a Capable and Ready Cybersecurity Workforce (Figure 1).

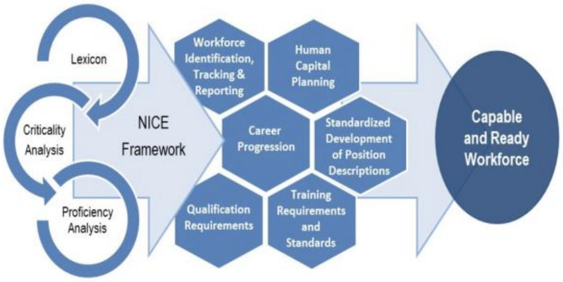

Lexicon
Criticality Analysis
Proficiency Analysis
NICE Framework
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Workforce

Figure 1: Building Blocks for a Capable and Ready Workforce (Newhouse, 2017)

The National Security Agency's (NSA) Cryptologic School manages the National Centers of Academic Excellence in Cybersecurity (NCAE-C). NCAE-C is supported by multiple federal partners to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- Establish standards for cybersecurity curriculum and academic excellence,
- Includes competency development among students and faculty,
- Values community outreach and leadership in professional development,
- Integrates cybersecurity practice within the institution across academic disciplines, and
- Actively engages in solutions to challenges facing cybersecurity education (NCAEC, N.D.)

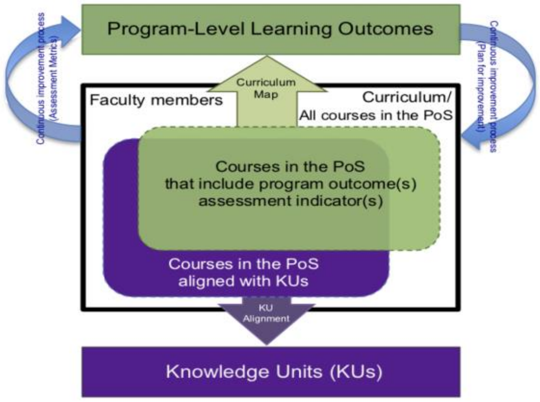

Program-Level Learning Outcomes
Continuous improvement process (Assessment Metrics)
Continuous improvement process (Plan for improvement)
Curriculum Map
Faculty members
Curriculum/ All courses in the PoS
Courses in the PoS that include program outcome(s) assessment indicator(s)
Courses in the PoS aligned with KUs
KU Alignment
Knowledge Units (KUs)

Figure 2: NCAE-C Program of Study (PoS) Evaluation Conceptual Model (NCAEC, 2021)

Academic institutions may be awarded one of three designations based on various criteria: Cyber Defense, Cyber Research, and Cyber Operations. These academic institutions align their curriculum map to learning outcomes which align with the NIST / NICE Framework. Additionally, the NCAE-C requires that designated programs integrate a continuous improvement process to ensure that the curriculum evolves with the state of cybersecurity outlined in Figure 2.

5. CURRICULUM

The National Cybersecurity Training and Education (NCyTE) Center aims to advance cybersecurity education in the U.S. by investing in technological innovation, resources, professional development, and tools to support faculty, community colleges, and the workforce pipeline of tomorrow (About NCyTE, 2021). NCyTE provides resources for faculty, industry, and centers of academic excellence. Additionally, NCyTE provides cybersecurity curriculum consisting of dozens of modules across a variety of topics including Advanced Placement Computer Science Principles; Cybersecurity, Cyber Intelligence Curriculum, Critical Infrastructure Security & Resilience (CISR), Critical Infrastructure Cybersecurity, Applied Cryptography, Cyber Threats & Counter Measures, Responsible Software Development, Secure Scripting, Cybersecurity and Society, Cybersecurity Principles, and Securing Data From Risk (Cybersecurity Curriculum, 2021). NCyTE supplements this content by providing webinar series, workshops, and resources to run camps and other activities.

Similarly, Cyber.org's goal is to empower educators as they prepare the next generation to succeed in the cyber workforce and ensure that every K-12 student receives foundational and technical cybersecurity knowledge and skills (Cyber.org, 2021). Cyber.org released the first national K-12 cybersecurity learning standards focused on computing systems, digital citizenship, and security. Cyber.org has thousands of hours of curriculum broken down by grade level across career and technical education, computer science, cybersecurity, engineering, humanities, math, robotics and coding, and science. Additionally, cyber.org provides professional development to empower educators.

Two additional resources for obtaining and sharing resources and curriculum are the Centers of Academic Excellence in Cybersecurity Resource Directory (CARD) (CARD, 2021) and the Cybersecurity Labs and Resource Knowledge

Base (CLARK) (CLARK, 2021) to support educational institutions. CARD is a general resource directory that contains reports, grant deliverables, conference resources, competition frameworks, workshops and materials, and additional resources to support labs and summer camps. CLARK is focused on the development and sharing of cybersecurity curriculum. Content is broken down by topic (22 topic areas), education level (Elementary-, Middle-, High-School, Undergraduate, Graduate, Post-Graduate, Community College, and Training), and length (Nanomodule – 1 hour or less, Micromodule – 1 – 4 Hours, Module – 4 – 10 Hours, Unit – Over 10 Hours, Course – 15 Weeks) (CLARK, 2021).

6. CURRENT SOLUTIONS

The developed curriculum and support by the U.S. government appears to support solving the cybersecurity education and workforce development problem. NIST / NICE and NCAE-C outline standards; and NCyTE, Cyber.org, CARD, and CLARK provide hundreds of hours of curriculum, content, workshops, and webinars to empower educators. Despite this, the cybersecurity education and workforce development problems continue to exist. There are a few reasons for this. First, focused cybersecurity education and training mostly begins at the collegiate level and is siloed. Second, industry does not know what KSAs they need for the roles they are trying to fill. This is evident by job ads where skills, position levels, and pay are incongruent. Finally, aligning with the movement of cybersecurity education into the K-12 space, "Cyber-Safety" must be implemented seemingly at birth considering that internet connected toys and devices enter children's lives early. This section outlines previous work that addresses Cyber-Safety, Cyber-Education, and Cyber-Skills designed to improve capabilities of the cyber workforce and reduce risk.

Cyber-Safety

Cyber-Safety initiatives can reduce the nation's susceptibility to cybercrime and reduce risk. Cyber criminals typically prey on the weakest or most vulnerable; therefore, steps must be taken to educate and prepare those systems and populations at the greatest risk. Cyber-Safety is applicable to everyone. People are introduced to technology at different points of their lives and their fluency with technology depends on many factors. Cyber-safety should be introduced at a young age considering technology will be part of their entire lives. Children are taught how to safely navigate their world from a young age. This includes how to safely cross the street, not touching sharp or hot objects, wearing protective devices like helmets and seat belts, fire safety, stranger safety, and water safety. The research, content, and application of cyber-safety for children birth to 5 years remains under researched and limited in practice (Edwards, 2021). Additionally, the long term impacts of identity theft with this population may not be understood for years.

Similarly, the elderly population, those aged 65 years or more, are at increased risk. Cybercrime against elderly fits into two general categories of fraud committed by strangers targeting investments, charity contributions, and loans and mortgages and financial exploitation by relatives and caregivers (Arfi, 2013). According to the FBI (Munanga, 2019), older adults are prime candidates of these crimes due to their credit history and when cognitive decline necessitates the need for others to manage their finances. This cohort typically lacks the familiarity with technology that other generations have. Additionally, they are less likely to be cognizant of cybersecurity threats and lack the experience to identify fraud in the digital space. The Center for Internet Security (Aliperti, 2021), Cyber Patriot CyberGenerations Program (Cyberpatriot 2022), the Cybersecurity & Infrastructure Security Agency (CISA, 2022), and various industry and government partners offer training and resources to support the elderly. Despite the increased awareness, training, and available resources; the financial damage for seniors is estimated at $1.68 billion annually (Abbate, 2021).

Cyber-Education

As previously mentioned, there are seven common cybersecurity functions and 33 specialized areas as defined in the NICE Framework. These areas span from the non-technical to the deeply technical. Additionally, individuals from all backgrounds leverage cyber resources during daily life. Thus, Cyber-Education content must be tailored to the audience. Research conducted at Southeastern Louisiana University determined that survey participants not in a technology-focused major are at a disadvantage when it comes to general cybersecurity knowledge and privacy practices (McNulty, 2021).

Similarly, Cyber-Education must be integrated into all education levels. The curriculum must be tailored to be digestible and applicable for each age / education level. This requires a multi-level, multi-discipline approach that provides a level of cybersecurity education that is appropriate for an individual's role in society as depicted in Figure 3.

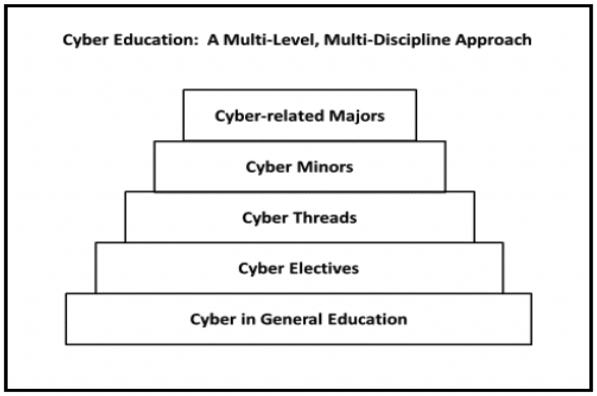

Cyber Education: A Multi-Level, Multi-Discipline Approach
Cyber-related Majors
Cyber Minors
Cyber Threads
Cyber Electives
Cyber in General Education

Figure 3: Multi-Level, Multi-Discipline Cyber Education Approach (Sobiesk, 2015)

Additionally, cybersecurity educational programs vary in content, application, breadth and depth, and integrated labs with hands-on learning. The work of NICE, NCyTE, Cyber.org, and others seeks to ensure that graduates at various levels have the tangible skills necessary to secure and thrive in the cybersecurity profession. Additionally, there are approximately 80 CAE-R, 22 CAE-CO, and over 200 CAE-CD designated schools (CAE, 2021). These schools meet or exceed the requirements set by the National Security Agency and are reviewed by peer institutions to ensure consistency and quality across schools.

Further, cybersecurity education programs focusing on high school students are being developed. Regions Investing in the Next Generation (RING) is an online high school cybersecurity course that offers content for students and schools without existing cybersecurity programs which will officially launch in 2022 (RING, 2022). RING allows students to achieve high school credit in participating states. Also, RING provides networking and professional development through the RING student organization. Additionally, Cyber.org facilitated collaboration among key stakeholders to develop and publish a set of K-12 cybersecurity learning standards. These standards center on computing systems, digital citizenship, and security to ensure that students have a foundational understanding of cybersecurity and the skills and knowledge to pursue cybersecurity careers (Cyber.org, 2022).

Cyber-Skills

People starting their cybersecurity careers have three primary methods for developing skills necessary to increase employability. These are learning skills through self-study or other experiential learning, completing industry certifications, or gaining a related degree (Marquardson, 2018). This section focuses on the complementary skill development of certifications, On-the-Job Training (OJT) and Internships / Apprenticeships, and experiential learning.

Certifications

Research indicates that certifications are important since they build confidence in cybersecurity professionals, validate their level of knowledge and skills versus untrained employees, and can execute their assigned tasks more consistently (James, 2019). Since 1989, Information Technology certifications have been introduced to reinforce and assess individuals or groups (Jarocki, 2019). Certifications are generally broken down into vendor-neutral and vendor-specific. Certification vendors factor in the current threat landscape, changing technologies, workforce needs, industry standards, and government and regulation to develop and maintain the certifications depicted in Figure 4.

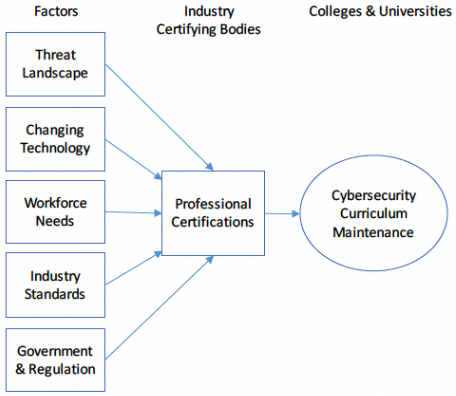


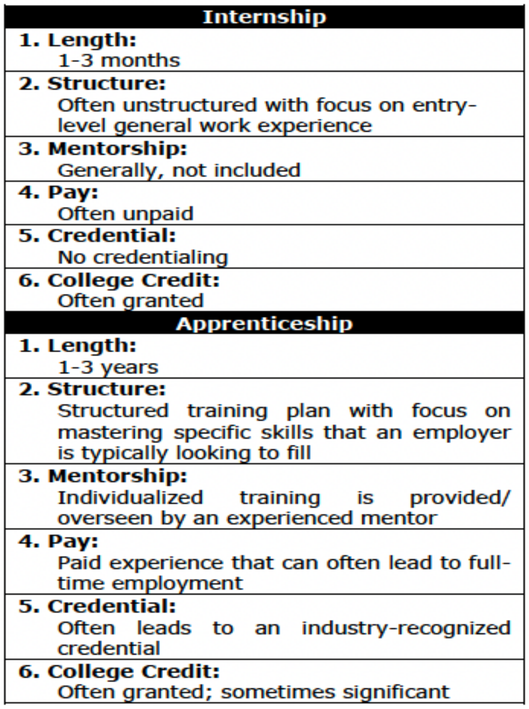
Figure 4: Factors Impacting the Maintenance of Cybersecurity Certifications (Knapp, 2017)

There are hundreds of cybersecurity certifications provided by many organizations including Computing Technology Industry Association (CompTIA), International Council of Electronic Commerce Consultants (EC-Council), Global Information Assurance Certification (GIAC), ISACA, and the International Information Systems Security Certification Consortium (ISC2). The 2022 Cybersecurity Certification Roadmap (Jerimy, 2022) maps over 400 certifications across various cyber domains of Communication and Network Security, Information Assurance Management, Security

Architecture and Engineering, Asset Security, Security and Risk Management, Security Assessment and Testing, Software Security, and Security Operations. (Appendix B).

On-the-Job-Training / Apprenticeships / Internships / Experiential Learning

Cybersecurity degree programs obtain a competitive advantage based on the amount of "hands-on" content within the curriculum considering industry requires a significant amount of skills-based training (Glantz, 2021). Complementing this "hands-on" content embedded into education programs and certifications is On-the-Job Training (OJT), internships / apprenticeships, and experiential learning. Internships and apprenticeships allow potential employees to gain, develop, and refine their cybersecurity skills while providing insight into the career field. Access and value to these opportunities varies. Figure 5 outlines key differences between these two opportunities.



Internship
1. Length: 1-3 months
2. Structure: Often unstructured with focus on entry-level general work experience
3. Mentorship: Generally, not included
4. Pay: Often unpaid
5. Credential: No credentialing
6. College Credit: Often granted
Apprenticeship
1. Length: 1-3 years
2. Structure: Structured training plan with focus on mastering specific skills that an employer is typically looking to fill
3. Mentorship: Individualized training is provided/ overseen by an experienced mentor
4. Pay: Paid experience that can often lead to full-time employment
5. Credential: Often leads to an industry-recognized credential
6. College Credit: Often granted; sometimes significant

Figure 5: Internship and Apprenticeship Differences (Stoker, 2021)

Although the experiences vary, the results are positive considering those that complete at least one internship receive 16% more job offers than those who don't and 94% of individuals that complete an apprenticeship program retain employment (Goin, 2021).

Finally, experiential learning in the form of self-study, participating in summer camps, and participating in "capture-the-flag" competitions can augment other skill development opportunities. For example, the Air Force Association (AFA) sponsored CyberPatriot program has evolved from a defense based cybersecurity competition to include curriculum to support elderly (Cybergenerations), educators (Elementary School Cyber Education Initiative (ESCEI)), and an information campaign through their CyberPatriot Literature Series. The CyberPatriot National Youth Cyber Defense competition challenges teams of high school and middle school students to find and fix cybersecurity vulnerabilities in virtual operating systems (CyberPatriot, 2021). Alternatively, the GenCyber program provides cybersecurity experience for students and teachers at the secondary level. GenCyber focuses on:

- Increasing awareness of K-12 cybersecurity content and career opportunities,
- Increase student diversity in cybersecurity college and career readiness pathways, and
- Facilitate teacher readiness within a teacher learning community (GenCyber, 2022).

Additionally, the National Cyber League (NCL) bridges the gap between high school and college students by providing a performance-based, learning-centered cybersecurity competition providing practical cybersecurity challenges competitors are likely to face in the workplace (NCL, 2021). Alternatively, TryHackMe (TryHackMe, 2021) and HacktheBox (HTB, 2021) provide platforms for gaining hands-on cybersecurity skills.

7. A BETTER APPROACH

As previously stated, a unified approach incorporating the various learning opportunities must be developed to solve the cybersecurity workforce problem. An example is the Cross-Boundary Cyber Education Design (Glantz, 2020) which builds upon the Multi-Level, Multi-Discipline Cyber Education Approach by adding curricular design insights from cyber master's degree programs and cyber certification offerings (Figure 6).

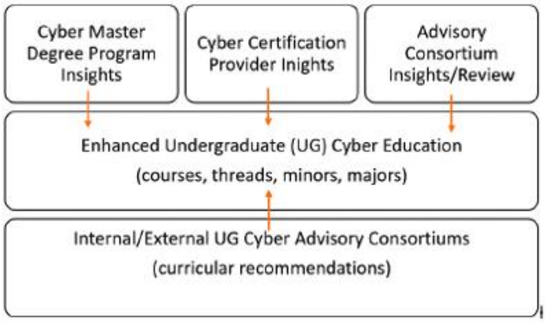

Cyber Master Degree Program Insights
Cyber Certification Provider Insights
Advisory Consortium Insights/Review
Enhanced Undergraduate (UG) Cyber Education
(courses, threads, minors, majors)
Internal/External UG Cyber Advisory Consortiums
(curricular recommendations)

Figure 6: Cross-Boundary Process Guiding Undergraduate Research (Glantz, 2020)

Although a more inclusive view of developing undergraduate education, it still does not include K-12 education and cyber safety. Additionally, government initiatives, legislation, and regulation can drive or limit innovation in the education space. This must be considered.

A "CyberEducation-by-Design" approach should be developed to incorporate the various components previously discussed from: cyber-safety, cyber-education, and cyber-skills. This should include the following key components:

- Curriculum designed and applicable to the age group and appropriate for the individual's roles in society.
- Curriculum designed to be accessible and inclusive. This may include Diversity, Equity, and Inclusion (DEI), socio-economic status of the individual and the school district, and several factors.
- Individuals should be able to inject themselves into the cybersecurity talent pipeline at any point. Many incoming cybersecurity professionals transfer from other careers, upskill within Science, Technology, Engineering, and Math (STEM) fields, or find non-traditional paths to cybersecurity.
- A holistic approach incorporating safety, education, certifications, and experiential learning should work synergistically to remove silos.
- When possible, clearly articulated pathways should be developed.

Figure 7 maps these various aspects grounded in standards based curriculum at various grade levels. Depending on the school and school district, the titles and age ranges for the various school levels may vary slightly. The center of the diagram is focused on the educational levels and associated age groups at those educational levels. This also aligns with formal learning activities which could incorporate the content and curriculum provided by Cyber.org, CLARK / CARD, Regions Investing in the Next Generation (RING) as that material aligns with formal learning activities. The elements above the educational aspects integrate safety concepts, camps, and competitions accessible at those ages / educational levels. The elements below focus on experiential learning and skill development aligned with workforce development. These elements align with non-formal and informal learning activities which complement student development during formal learning.

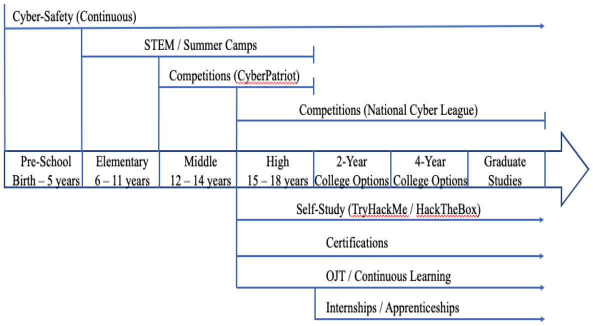

Cyber-Safety (Continuous)
STEM / Summer Camps
Competitions (CyberPatriot)
Competitions (National Cyber League)
Pre-School
Birth – 5 years
Elementary
6 – 11 years
Middle
12 – 14 years
High
15 – 18 years
2-Year
College Options
4-Year
College Options
Graduate
Studies
Self-Study (TryHackMe / HackTheBox)
Certifications
OJT / Continuous Learning
Internships / Apprenticeships

Figure 7: CyberEducation-By-Design Model

The Cybersecurity Education Pathway Table provided in Appendix C demonstrates a pathway that maps cybersecurity curriculum and certifications from a high school to an associated community college to a four-year institution. For the purposes of this mapping, general education courses are not included. Additionally, the experiential learning aspects outlined in this paper can be programmed into the curriculum to support learning objectives and skill development.

This course sequence and pathway is based on an existing pathway from Basha High School's Institute of Cyber Operations and Networking (Basha, 2022), Chandler Gilbert Community College's Associate of Applied Science in Cybersecurity (CGCC, 2022), and the University of Arizona's Cyber Operations program (Cyber Operations, 2022). The pathway provides a seamless educational experience through the educational levels. Opportunities for mentorship, camps, experiential learning, professional development, internships, and employment are integrated throughout. These opportunities are provided by local, state, and national partners.

The inclusion of the specific elements within the CyberEducation-By-Design Model were based on the literature review and the review of the Basha High School program previously mentioned. This is not meant to be an inclusive list of activities and further research into specific examples and outcomes will be explored in future research.

8. CONTRIBUTIONS

Contributions of this paper include (1) a historical review of government legislation that recognize and attempt to address cybersecurity education and deficiencies within the cybersecurity workforce, (2) an outline standards organizations including NIST / NICE and NCAE-C, and (3) an outline of the available curriculum provided by NCyTE, Cyber.org, CLARK, and CARD. Additionally, a systematic literature review was conducted to identify initiatives being implemented to address the cybersecurity education and workforce development problem. This review focused on cyber-safety, cyber-education, and cyber-skills. Most importantly, a "CyberEducation-by-Design" approach was introduced. This design maps various aspects of cybersecurity education and training holistically. This model will require further refinement and additional overlays can be introduced and integrated to improve upon the initial design. Specifically, extending the timeline beyond graduate studies or branching a pathway for non-traditional learners could enhance the model. Additionally, articulated pathways can aid students in selecting cybersecurity as a career and understand their options earlier.

9. LIMITATIONS AND FUTURE RESEARCH

Multiple curriculum resources were discussed in this paper. The focus was on vetted, open source resources that are general enough to allow for adoption by a variety of education institutions. This represents a fraction of the overall free and open source content available and does not include content provided by textbook publishers or paid content. Future research in this area could be more inclusive of these options and potentially map all resources available to provide a central repository for that information. CLARK and CARD attempt to do that but is limited in scope and scale. Further, most state standards focus on computer science and integrate cybersecurity concepts as an afterthought. Research and development of cybersecurity specific state standards could further the development and adoption of cybersecurity education programs at K-12.

Multiple elements were integrated into the proposed CyberEducation-by-Design model which were selected based on elements identified during the literature review and a review of the Basha High School Cybersecurity program. These elements could be further codified and aligned with informal and non-formal learning activities to generalize the activities for broader applicability. Further, the model itself will be continually refined. A qualitative research study will be conducted on existing cybersecurity programs at secondary education institutions to further identify critical program elements and refine the model. Data collection will inform the development of a framework for cybersecurity education programs at secondary education institutions.

Finally, funding was not explored in this study. There are many grant and scholarship opportunities for educators, students, curriculum development, and developing and hosting experiential learning opportunities. These range from individual awards to consortiums of multiple schools. Cataloguing these opportunities and making them accessible to stakeholders can address or improve many of the issues associated with cybersecurity education and workforce development discussed in this paper.

10. CONCLUSIONS

There continues to be hundreds of thousands of unfilled jobs within the United States and millions globally. Additionally, adversaries are rapidly building their cyber capabilities both in numbers and skills. Further, -as-a-Service capabilities allow adversaries to quickly execute attacks with limited or no preparation. Overcoming these things requires a holistic, agile, and innovative approach adopted by students, educators, employers, and governments.

Since President Reagan signed the Computer Security Act of 1987, presidents have taken a proactive stance on addressing the nation's cybersecurity issues through improved legislation including the National Security Strategy to Secure Cyberspace, Executive Order 13636 "Improving Critical Infrastructure Cybersecurity", implementing the Cybersecurity National Action Plan, Executive Order 13800 "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", the K-12 Cybersecurity Act, and others. These actions led to the development of NIST Special Publication 800-181 Workforce Framework for Cybersecurity (NICE Framework) and the NSA's National Centers of Academic Excellence in Cybersecurity (NCAE-C) standards. Additionally, in partnerships with these agencies and others, free and open source curriculum has been developed and catalogued by NCyTE, Cyber.org, CARD, and CLARK. These initiatives provide a foundation for addressing this national problem.

The literature review identified initiatives to address the cybersecurity education and workforce development problem focusing on three categories including cyber-safety, cyber-education, and cyber-skills. Cyber-safety identified the need for early and ongoing safety campaigns to ensure that all citizens have the knowledge and skills necessary to operate within their societal roles. Additional focus should be on the most vulnerable cohorts: infants, toddlers, and the elderly. Cyber-education reviewed the need for well-defined cybersecurity functions and job roles mapped to the required knowledge, skills, and abilities to meet those functions. These requirements help define the curriculum content. Additionally, cyber-education must be integrated into all education levels at the appropriate level for the learner in a multi-level, multi-discipline educational approach. Further, curriculum across educational institutions can vary greatly. Ensuring that schools are evaluated and meet certain content and quality standards is important. Finally, cyber-skill development in the form of certifications, On-the-Job-Training (OJT), apprenticeships, internships, and experiential learning were discussed.

Finally, a "CyberEducation-by-Design" model was introduced to address the need for curriculum to be integrated at all levels across disciplines that is appropriate for the learner. This curriculum must be accessible and inclusive. It also acknowledges that aspiring cybersecurity professionals inject themselves into the talent pipeline at different points on the spectrum and points in their lives. Cyber safety, education, certifications, and experiential learning should work synergistically and when possible, clearly articulated pathways should be developed. Although improvements can be made to this model, developing a repeatable, inclusive, and comprehensive model can greatly improve the cybersecurity posture of the nation.

11. REFERENCES

"A Massive Hacking Playground," (2021). Hack The Box. https://www.hackthebox.com/.

Abbate, P. (2021). Federal Bureau of Investigation Internet Crime Report 2021. Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

"About NCyTE," (2021). National Cybersecurity Training and Edcuation Center (NCyTE) Center. https://www.ncyte.net/about-us/about.

"About Us" (2021). Cyber.org. https://cyber.org/about-us, 2021.

Aliperti, M. (2021, June). How to Protect Seniors Against Cybercrimes and Scams. Center for Internet Security. https://www.cisecurity.org/insights/newsletter/how-to-protect-seniors-against-cybercrimes-and-scams.

Arfi, N. and Agarwal, S. (2013, June). Knowledge of Cybercrime among Elderly. International Journal of Scientifica & Engineering Research. https://www.researchgate.net/profile/Shalini-Agarwal-5/publication/242654499_Knowledge_of_Cybercrime_among_Elderly/links/0deec51cebeac0feef000000/Knowledge-of-Cybercrime-among-Elderly.pdf.

Armerding, T. (2017, January 31). Obama's cybersecurity legacy: Good intentions, good efforts, limited results. CSO Online. https://www.csoonline.com/article/3162844/obamas-cybersecurity-legacy-good-intentions-good-efforts-limited-results.html.

Basha High School (2022). Institute of Cyber Operations and Networking. Basha High School Cybersecurity Academy. https://www.cusd80.com/BHSCyber.

Biden, J. (2021, May 12). Executive Order on Improving the Nation's Cybersecurity. The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Brooks, K. (2021, May 21). U.S. has almost 500,000 job openings in cybersecurity. CBS News. https://www.cbsnews.com/news/cybersecurity-job-openings-united-states/.

Bush, G. (2003, February). The National Strategy to Secure Cyberspace. A White House Report. https://ciaotest.cc.columbia.edu/olj/gli/gli_nov2003/gli_nov2003k.pdf.

"CAE Institution Map," (2021). CAE In Cybersecurity Community. https://www.caecommunity.org/cae-map.

GCGG (2022). Associate in Applied Science in Cybersecurity. Chandler-Gilber Community College. https://www.cgc.edu/degrees-certificates/computer-and-information-technology/cybersecurity-3197-aas.

CIS (2021, March 15). The SolarWinds Cyber-Attack: What You Need to Know. Center for Internet Security. https://www.cisecurity.org/solarwinds/.

CISA (2020, October 28). Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastrucutre. Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov/executive-order-strengthening-cybersecurity-federal-networks-and-critical-infrastructure.

Clinton, B. (2000, February 16). President Clinton: Working to Strengthen Cybersecurity. The White House, White House at Work.

https://clintonwhitehouse4.archives.gov/WH/Work/021600.html.

Cluley, G. (2021, October 21). US Government warns of BlackMatter ransomware attacks against critical infrastructure. Tripwire. https://www.tripwire.com/state-of-security/security-data-protection/us-government-warns-of-blackmatter-ransomware-attacks-against-critical-infrastructure/.

Cyber Academy (2021). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Cyber Academy. https://cyberacademy.co/cybersecurity-talent-crunch-to-create-3-5-million-unfilled-jobs-globally-by-2021/.

Cyber Innovation Center and Cyber.org (2021). K-12 Cybersecurity Learning Standards. https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf.

Cyber Operations (2022). Bachelor of Applied Science in Cyber Operations. University of Arizona. https://cyber-operations.azcast.arizona.edu/.

CyberPatriot (2022). CyberGenerations – The Senior Citizens' Cyber Safety Initiative. Air Force Association. https://www.uscyberpatriot.org/Pages/Special%20Initiatives/CyberGenerations-Overview.aspx#:~:text=CyberGenerations%20%2D%2D%20the%20Senior%20Citizens,of%20a%20self%2Dpaced%20guide.

"CyberPatriot National Youth Cyber Education Program Competition Overview," (2021). Air Force Association. https://www.uscyberpatriot.org/competition/Competition-Overview/competition-overview.

"Cybersecurity Curriculum," (2021). NCyTE Center. https://www.ncyte.net/resources/cybersecurity-curriculum.

Cybersecurity & Infrastructure Security Agency (2022). CISA Cybersecurity Awareness Program Older American Resources. CISA. https://www.cisa.gov/publication/cisa-cybersecurity-awareness-program-older-american-resources.

Cyber Seek (2022, September 9). Cyber Seek Cybersecurity Supply and Demand Heat Map. Cyber Seek. https://www.cyberseek.org/heatmap.html.

"Cybersecurity Education Resource Directory," (2021). National Cryptologic Foundation. https://www.caeresource.directory/home.

"Cybersecurity Labs and Resource Knowledge-base," (2021). Clark Center. https://clark.center/home.

Edwards, S. (2021, June 14). Cyber-safety and COVID-19 in the early years: A research agenda. Journal of Early Childhood Research. https://journals.sagepub.com/doi/pdf/10.1177/1476718X211014908.

"FACT SHEET: Cybersecurity National Action Plan." (2016, February 9). Office of the Press Security, The White House. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

GenCyber (2022). Inspiring the Next Generation of Cyber Stars. GenCyber. https://www.gen-cyber.com/about/.

Glantz, E., Bartolacci, M., Naseredding, M., and Fusco, D. (2020). Cross-Boundary Cyber Education Design. SIGTE. https://doi.org/10.1145/3368308.3415374.

Glickman, D. (1988, January 8). H.R. 145 – Computer Security Act of 1987. Congress.gov. https://www.congress.gov/bill/100th-congress/house-bill/145.

Goin, A., Branter, C., Johnston, L., Rodriguez, R., and Hott, J. (2021). Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity. Idaho National Laboratory. https://inl.gov/wp-content/uploads/2021/09/3-CyberLeague-Whitepaper-Final-20210903.pdf.

Herjavec, R. (2019, July 17). Cybersecurity CEO: The History of Cybercrime, From 1834 to Present. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-ceo-the-history-of-cybercrime-from-1834-to-present/.

ISC2 (2021). A Resilient Cybersecurity Profession Charts the Path Forward, ISC2 Cybersecurity Workforce Study, 2021. International Information Systems Security Certification Consortium. https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

James, J. and Callen, J. (2019, October). Cybersecurity Certifications Matter. Issues in Information Security. https://www.researchgate.net/publication/338805856.

Jarocki, S. and Kettani, H. (2019). Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts. International Conference on Information Systems Engineering (ICISE). https://www.researchgate.net/publication/338506367_Examining_the_Efficacy_of_Commercial_Cyber_Security_Certifications_for_Information_Security_Analysts.

Jerimy, P. (2022, August). Security Certification Roadmap 2022. Paul Jerimy. https://pauljerimy.com/security-certification-roadmap/.

"Join 500k other learning Cybersecurity with TryHackMe," (2021). Try Hack Me. https://tryhackme.com/.

"K-12 Cybersecurity Act of 2021," (2021, October 8). 117th Congress Public Law No: 117-47, https://www.congress.gov/bill/117th-congress/senate-bill/1917/all-info.

Knapp, K., Maurer, C., and Plachkinova, M. (2017, December 12). Maintaining Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. Journal of Information Systems Education. http://jise.org/Volume28/n2/JISEv28n2p101.html.

Marquardson, J. and Elnoshokaty, A. (2018). Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs. Information Systems Education Journal. https://doi.org/10.48009/3_iis_2018_193-201.

McNulty, M. (2021). Cybersecurity Education for Non-Technical Learners. Beadle Scholar. https://scholar.dsu.edu/cgi/viewcontent.cgi?article=1365&context=theses.

Munanga, A. (2019, January 11). Cybercrime: A New and Growing Problem for Older Adults. Journal of Gerontological Nursing. https://doi-org.ezproxy3.library.arizona.edu/10.3928/00989134-20190111-01.

"National Centers for Academic Excellence in Cybersecurity," (N.D.). National Security Agency / Central Security Service. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

"National Centers of Academic Excellence in Cybersecurity CAE 2021: Proposed Designation Requirements and Application Process for CAE Cyber Operations," (2021, March). National Security Agency / Central Security Service. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-proposed_cae-co_designation_requirements.pdf.

Newhouse, W., Keith, S., Sribner, B., and Witte, G. (2017, August). NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf, August 2017.

Obama, B. (2013, February 12). Cybersecurity – Executive Order 13636. The White House. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636.

Obama, B. (2015). H.R.2029-694 – Cybersecurity Act of 2015. Senate.gov. https://www.intelligence.senate.gov/sites/default/files/legislation/Cybersecurity-Act-Of-2015.pdf.

Petersen, R., Santos, D., Smith, M., Wetzel, K., and Witte, G. (2020, November). NIST Special Publication 800-181 Rev. 1, Workforce Framework for Cybersecurity (NICE Framework). National Institute for Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1.

RING (2022). Regions Investing in the Next Generation (RING). https://caecommunity.org/initiative/k12-ring#:~:text=What%20is%20RING%3F,without%20an%20existing%20cybersecurity%20program.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., and Taylor, H. (2015, October 3). Cyber Education: A Multi-Level, Multi-Discipline Approach. SIGITE. http://dx.doi.org/10.1145/2656450.2656478.

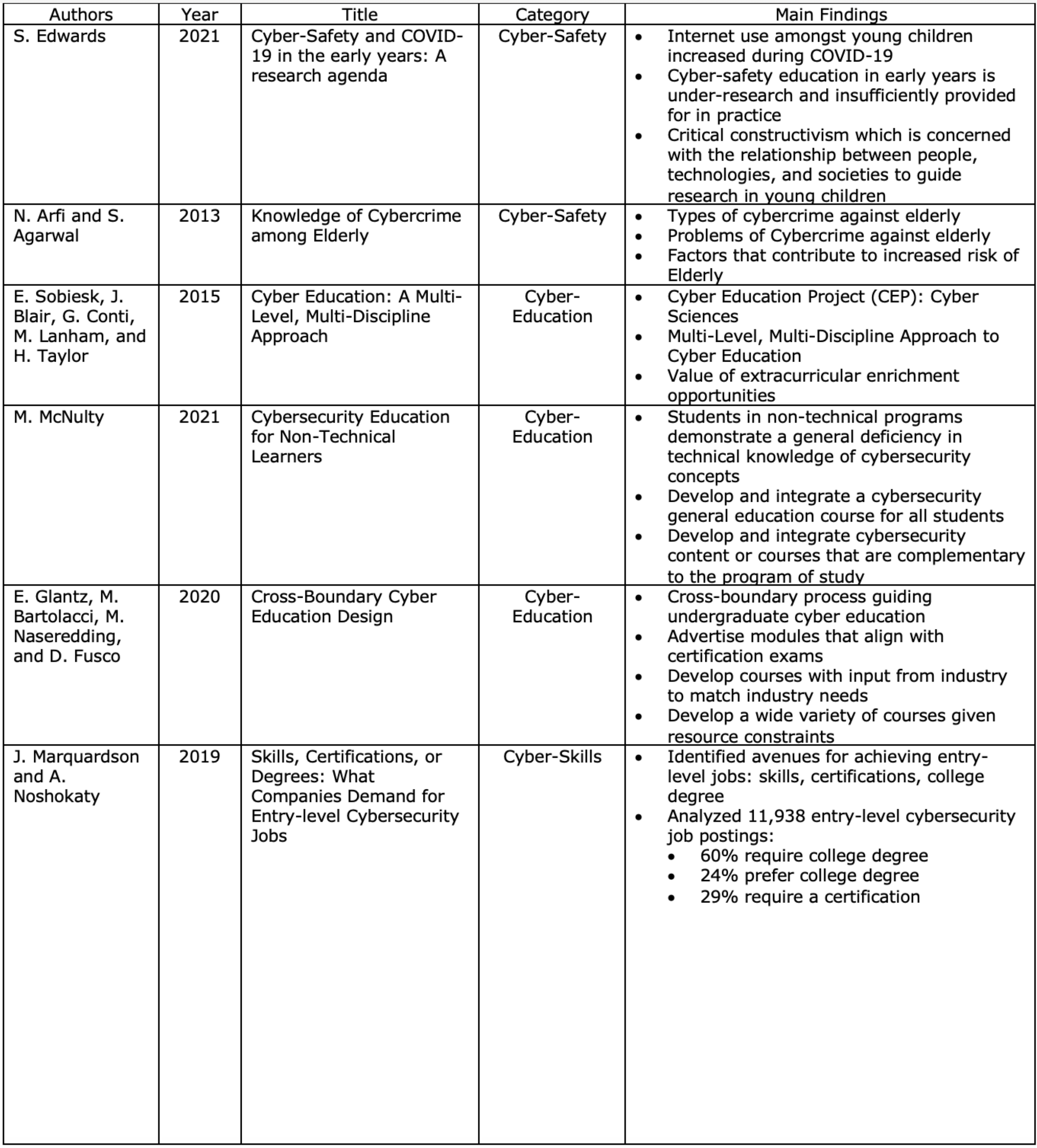
Stoker, G., Clark, U., Vanajakumari, M., and Wetherill, W. (2021, April). Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned. Information Systems Education Journal (ISEDJ). https://files.eric.ed.gov/fulltext/EJ1297604.pdf.

"The National Cyber League," (2021). Cyber Skyline. https://nationalcyberleague.org/.

Turton, W. and Mehrotra, K. (2021, June 4). Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg Cybersecurity. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password.

Weiner, S. (2021, July 20). The growing threat of ransomware attacks on hospitals. Association of American Medical Colleges https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals

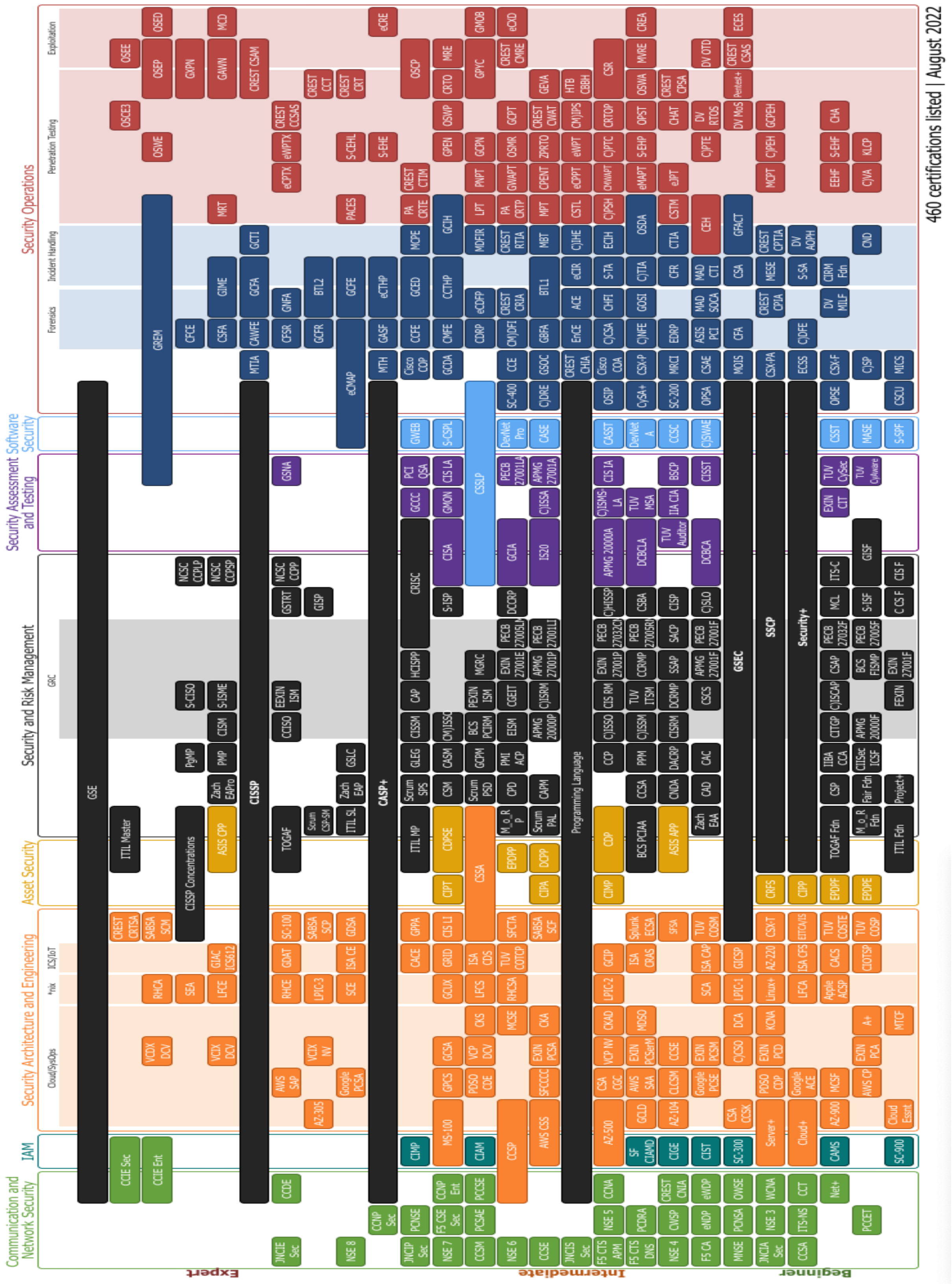
Appendix A: Systematic Literature Review Table



Authors	Year	Title	Category	Main Findings
S. Edwards	2021	Cyber-Safety and COVID-19 in the early years: A research agenda	Cyber-Safety	• Internet use amongst young children increased during COVID-19 • Cyber-safety education in early years is under-research and insufficiently provided for in practice • Critical constructivism which is concerned with the relationship between people, technologies, and societies to guide research in young children
N. Arfi and S. Agarwal	2013	Knowledge of Cybercrime among Elderly	Cyber-Safety	• Types of cybercrime against elderly • Problems of Cybercrime against elderly • Factors that contribute to increased risk of Elderly
E. Sobiesk, J. Blair, G. Conti, M. Lanham, and H. Taylor	2015	Cyber Education: A Multi-Level, Multi-Discipline Approach	Cyber-Education	• Cyber Education Project (CEP): Cyber Sciences • Multi-Level, Multi-Discipline Approach to Cyber Education • Value of extracurricular enrichment opportunities
M. McNulty	2021	Cybersecurity Education for Non-Technical Learners	Cyber-Education	• Students in non-technical programs demonstrate a general deficiency in technical knowledge of cybersecurity concepts • Develop and integrate a cybersecurity general education course for all students • Develop and integrate cybersecurity content or courses that are complementary to the program of study
E. Glantz, M. Bartolacci, M. Naseredding, and D. Fusco	2020	Cross-Boundary Cyber Education Design	Cyber-Education	• Cross-boundary process guiding undergraduate cyber education • Advertise modules that align with certification exams • Develop courses with input from industry to match industry needs • Develop a wide variety of courses given resource constraints
J. Marquardson and A. Noshokaty	2019	Skills, Certifications, or Degrees: What Companies Demand for Entry-level Cybersecurity Jobs	Cyber-Skills	• Identified avenues for achieving entry-level jobs: skills, certifications, college degree • Analyzed 11,938 entry-level cybersecurity job postings: • 60% require college degree • 24% prefer college degree • 29% require a certification

J. James and J. Callen	2018	Cybersecurity Certifications Matters	Cyber-Skills	• Certifications matter: Confidence, Validation, Execution • Cybersecurity certifications can increase KSAs and give students an edge when applying for jobs • Co-curricular activities such as competitions, journals, webinars, and seminars can enhance KSAs
S. Jarocki and H. Kettani	2019	Examining the Efficacy of Commercial Cyber Security Certifications for Information Security Analysts	Cyber-Skills	• Value and Effectiveness of cybersecurity certifications • Research is limited on efficacy of commercial incident response cyber security certifications in selecting potential candidates
K. Knapp, C. Maurer, and M. Plachkinova	2017	Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance	Cyber-Skills	• Factors impacting the maintenance of cybersecurity certifications • Appropriateness of using certifications for curriculum shaping • Experiential Learning and Capstone Courses
G. Stoker, U. Clark, M. Vanajakumari, and W. Wetherill	2021	Building a Cybersecurity Apprenticeship Program: Early-Stage Success and Some Lessons Learned	Cyber-Skills	• NICE Working Group on Apprenticeships • Cyberstart Apprenticeship • Cybersecurity Youth Apprenticeship Initiative
A. Goin, C. Branter, L. Johnston, R. Rodriguez, and J. Hott	2021	Idaho Cyber Heroes: Helping Individuals Navigate Career Pathways in Cybersecurity	Cyber-Skills	• Increasing Career Awareness in High Schoolers • Requirements and Barriers for a Career in Cybersecurity • Benefits of Internships and Apprenticeships • Lack of Diversity in the Cybersecurity Workforce

Appendix B – Certification Table



Appendix C – Cybersecurity Education Pathway Table

High School	**Community College**	**4-Year Institution**
• Survey of Computer Information Systems • Computer Hardware & Support* • Operating System Configuration * • Linux Operating System / Red Hat SysAdmin I • Introduction to Networks • AWS Cloud Foundations • Linux SysAdmin / Red Hat SysAdmin II • Information Security Fundamentals** • Python Programming • Ethics in Information Technology	• Ethical Hacking & Network Defense • Computer Information Systems • Internship / Special Project • Computer Forensics Foundations • Advanced Computer Forensics	• Computational Thinking & Doing • Introductory Methods of Network Analysis • Cyber Ethics • Introduction to Cyber Operations** • Active Cyber Defense • Cyber Threat Intelligence • Violent Python • Cyber Threat Intelligence • Cyber Warfare • Additional Elective Course
* Maps to CompTIA A+ Certification ** Could map to Security+ Certification / Partial Preparation		

Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution

Geoff Stoker
stokerg@uncw.edu

Jeff Greer
greerj@uncw.edu

Ulku Clark
clarku@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28412 USA

Christopher Chiego
cchiego@csum.edu
California State University Maritime Academy
Vallejo, CA 94590 USA

Abstract

The maritime industry, with its economically and strategically important role and critical infrastructure, appears to have a cybersecurity posture that lags other sectors (Akpan et al., 2022; Heering et al., 2021; National Academy of Public Administration, 2021). This lag is exacerbated by the current cybersecurity workforce shortage (Cyber Seek, 2022) which likely impacts maritime as much as all other industries. In this paper, we review the state of cybersecurity education within the maritime community and consider the possible value that cybersecurity students from non-maritime education and training (MET) institutions could bring to bear on maritime cybersecurity. We explore what additional knowledge these students might need in order to be ready to enter the maritime cybersecurity workforce and readily contribute.

Keywords: Cybersecurity, Maritime, Education

1. INTRODUCTION

International trade relies heavily on maritime operations. Both the International Maritime Organization (IMO, 2021b) and the United Nations (UN Conference on Trade and Development, 2021) estimate that 80+% of the world's trade by tonnage moves across the water. Like other industries and parts of the world economy, the maritime community is in the midst of significant *intelligent* digitally driven change as part of the Fourth Industrial Revolution (4IR) or Industry 4.0 (Schwab, 2017).

These changes are many and range across a broad spectrum – from the emergence of *smart* ports (Figure 1) to their full integration into the global supply chain (Figure 2, Zarzuelo et al., 2020) to the autonomous navigation of ships when underway (Noel et al., 2019). The digital footprint (Figure 3) spreads deep and wide throughout ships, ports, terminals, crew devices, etc., in a non-uniform and inconsistent manner across maritime operations worldwide (International Association of Ports and Harbors [IAPH], 2020).

While the addition of digital systems and the digitization of the many existing physical systems involved in maritime operations often leads to efficiencies that save money, reduce time, increase safety, and lessen environmental impact, the shift also creates new risks as these digitized systems are more exposed to potential cyber-attacks. While the potential risk of cyber-attack to maritime operations has been recognized for several decades, even being used as a Hollywood plot device before the turn of the millennium (de Bont, 1997), the industry has faced challenges in responding to the cybersecurity threat (Akpan et al., 2022; Caponi & Belmont, 2015; Chang et al., 2019; DiRenzo et al., 2015; Gliha, 2017; National Academy of Public Administration, 2021; Pyykkö, 2020; U.S. Government Accountability Office, 2014).

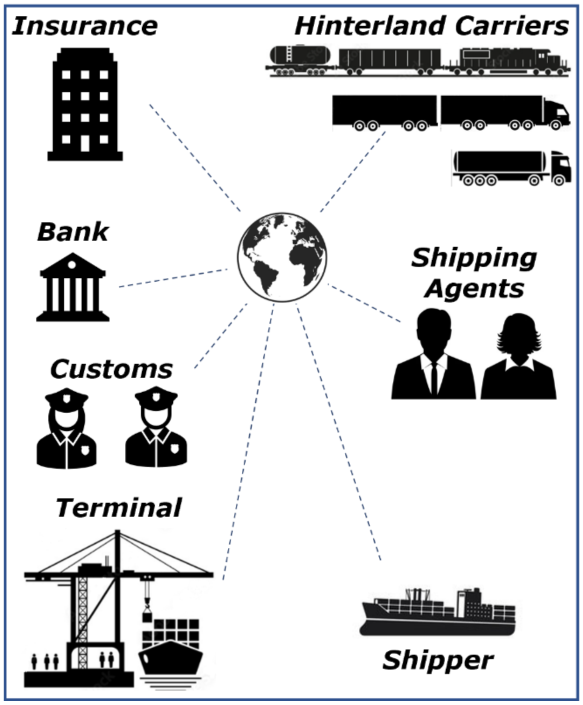


Figure 1 – stylized view of a smart port

The maritime industry encompasses almost everything connected to oceans, seas, and waterways including ports, shipyards, terminals, fishing, aquaculture, seafood processing, and many more areas. However, the focus of this paper is primarily around shipping transport, terminals, ports, and other aspects of the international shipping trade.

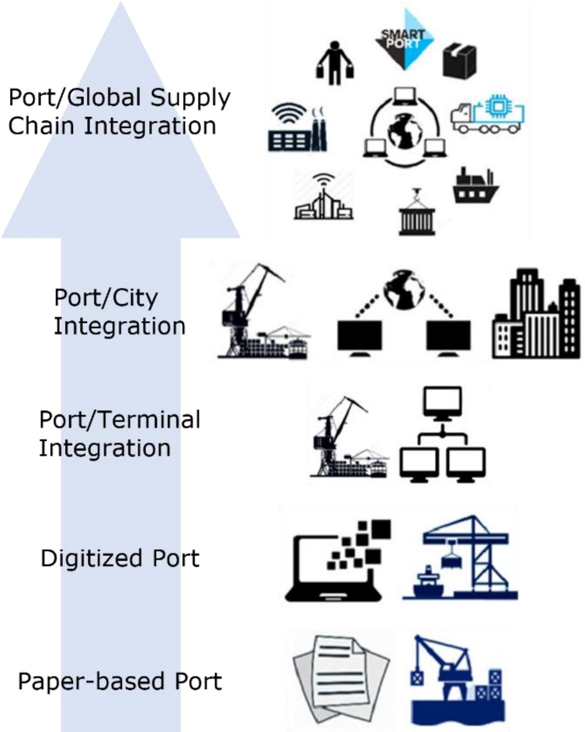
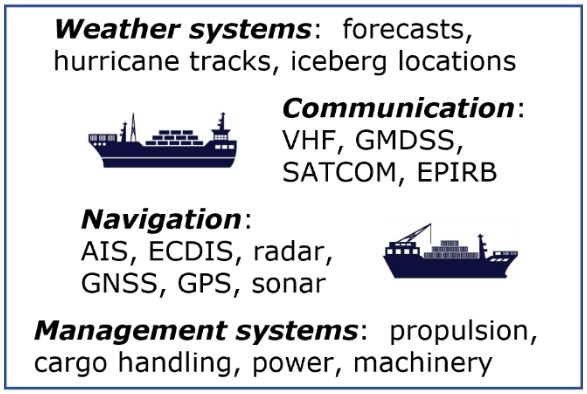

Port/Global Supply Chain Integration
SMART PORT
Port/City Integration
Port/Terminal Integration
Digitized Port
Paper-based Port

Figure 2 – Evolution of local, regional, global port operations (modified Fig. 1. de la Peña Zarzuelo et al., 2020)

Several major cyber-attacks in the 2010s focused the attention of the maritime industry on the critical importance of cybersecurity. In 2017, shipping industry leader Maersk saw its systems infected by the NotPetya malware, which nearly brought down the company's entire network. Thanks to a fortunately-timed disconnected computer with key data, Maersk was able to eventually reboot its network, albeit at a cost of disruptions estimated to have cost $300 million.



Weather systems: forecasts, hurricane tracks, iceberg locations

Communication: VHF, GMDSS, SATCOM, EPIRB

Navigation: AIS, ECDIS, radar, GNSS, GPS, sonar

Management systems: propulsion, cargo handling, power, machinery

Figure 3 – sample of systems in maritime operations (acronym list Appendix A)

Additional attacks in 2018 on China Ocean Shipping (COSCO) Group and in 2020 on a wide range of other maritime targets further confirmed the threats to the networks of large shipping companies (Loomis et al., 2021). Whole supply chains were impacted by these attacks, some of which were targeted at the industry specifically while others stemmed from accidental infection with malware.

Other industry vulnerabilities have also been targeted by hackers in recent years, including those found in the network at the port of Antwerp in 2013 which was infiltrated to facilitate drug smuggling (Loomis et al., 2021) and a German ship's navigation system which was remotely hacked in 2017 while transiting the Red Sea. Experimental hacking demonstrations have also underscored the vulnerabilities of the maritime domain, which presents many different avenues for potential cyberattacks (Demchak and Thomas, 2021).

Despite this wide range of vulnerabilities across many parts of the industry, the maritime sector is finding it difficult to recruit a maritime-focused cybersecurity workforce (Satira, 2021). As with other industries, the maritime community is feeling the impact of this cybersecurity workforce shortage despite the earnest efforts of governments, businesses, and academia to mitigate the problem. In early 2021, the White House announced (O'Brien, 2021) the release of the National Maritime Cybersecurity Plan which included a section prioritizing the creation of a maritime cybersecurity workforce that tasked the Department of Homeland Security (DHS) and the United States Coast Guard (USCG) with developing more career paths for maritime cybersecurity in both the private and public sectors (White House, 2020). In an October 2021 report on the future of Maritime Cybersecurity, the Atlantic Council noted that, "There is a pressing need to create a cybersecurity-capable workforce, ensuring cyber literacy among the next generation of mariners and operators," (Loomis et al., 2021, p. 36) and counseled for collaboration among academia, the federal government, and international maritime organizations to encourage cybersecurity education. As we discuss below, however, there are major gaps in the resources and opportunities available to make this happen.

Among the education community, the cybersecurity area has received increasingly accelerated attention over the past 25+ years. Efforts to create and bolster cybersecurity-related offerings have been encouraged by initiatives like the National Security Agency (NSA) administered National Centers of Academic Excellence in Cybersecurity (NCAE-C) Program begun in 1999 (Center of Academic Excellence in Cybersecurity Community, 2022b), the Joint Task Force (JTF) on Cybersecurity Education launched in 2015 that resulted in the development of the 2017 cybersecurity (CSEC2017) curricular guidelines (JTF, 2022), and the 2018 approval by the Accreditation Board for Engineering and Technology (ABET) of program-specific criteria for cybersecurity at the baccalaureate level (ABET, 2022a).

The NCAE-C currently has 389 institutions (Center of Academic Excellence [CAE] in Cybersecurity Community, 2022a) participating as a CAE in Cyber Defense (CAE-CD), Cyber Operations (CAE-CO) and/or Cyber Research (CAE-R) and ABET currently lists 26 institutions with accredited cybersecurity 2-yr or 4-yr programs (ABET, 2022b).

The maturing curricular offerings for cybersecurity generally and the current need in the maritime community for more cybersecurity expertise specifically motivated the writing of this paper and the consideration of the questions:

- Can undergraduate students studying cybersecurity at non-MET institutions enter the maritime cybersecurity workforce after graduation and readily contribute?
- To better prepare students for maritime industry participation, what might a curriculum track include to provide some maritime-specific cybersecurity focus?

In section 2 of this paper, we conduct a literature review of maritime cybersecurity education; section 3 investigates the common touch points between cybersecurity presented within the maritime community and that presented in non-MET cybersecurity programs; section 4 explores potential additions to non-MET cybersecurity programs to make students more maritime workforce ready; in section 5 we elaborate on one of the recommendations in section 4; section 6 concludes.

2. STATE OF MARITIME CYBERSECURITY EDUCATION

Within the maritime community, there are active efforts to improve the level of cybersecurity knowledge and practice like the IMO's adopting resolution MSC.428(98) on Maritime Cyber Risk Management in Safety management Systems (IMO, 2017) and the International Chamber of

Shipping (ICS) publishing of The Guidelines on Cyber Security Onboard Ships (ICS, 2021).

There are MET-adjacent institutions with notable cybersecurity expertise. For example, the United States Naval Academy (USNA) is both a member of the NCAE-C Program as well as accredited by ABET (ABET, 2022a; USNA, 2020) with their cyber operations program, and the United States Coast Guard Academy (USCGA) is currently seeking ABET accreditation for their cyber systems program (USCGA, 2022). However, at METs across the globe, there are indications of cybersecurity education gaps.

Burke and Clott (2016), due in part to increasing automation and the evolution of autonomous ship operation, saw a need and argued for "significant education in information technology with an emphasis on cyber security for ship designers, ship operators, all shoreside personnel" (p. 5). Ahvenjärvi et al. (2019) conducted a review of the International Convention on Standards for Training, Certification and Watchkeeping for Seafarers (STCW) and a survey of members from the International Association of Maritime Universities (IAMU) and concluded that both cybersecurity and cyber safety need to be better addressed in MET.

Alop (2019) examined the challenges posed to maritime education by the rapidly unfolding digital 4IR and concluded there is a need to change the paradigm. A survey of maritime professionals was conducted by Alcaide and Llave (2020), Sep-Dec 2018, to ascertain the mariners' level of cybersecurity knowledge. With 102 usable responses, they claimed the results indicated that "the lack of knowledge of maritime experts consulted exceeds 75%, where it is essential to highlight, among other topics: procedures (detect, act, communicate, recover, etc.); simulacra [drills]; cyber security/threats" (p. 553).

Through review of teaching materials and interviews with personnel at four MET institutions, Bacasdoon (2021) found that while cybersecurity was being taught, the topics, degree of depth, and modality differed considerably from one MET institution to the next. He developed a framework within which cybersecurity education and training could be effectively presented to seafarers. Bacasdoon also found, via a survey with 403 results, that seafarers generally perceived the MET institution cybersecurity topics being covered to be needed and considered important to the successful execution of their jobs.

In November 2021, the National Academy of Public Administration published a largely critical report assessing the U.S. Merchant Marine Academy (USMMA) that provided 67 recommendations to position USMMA to better handle the future challenges of functioning in an increasingly complex operating environment. Included was the recognition that "the maritime workforce of the future will need proficiency in data science, machine learning, and cybersecurity;" (p. 73).

Heering, et al. (2021), examining published maritime cybersecurity research on MET programs for seafarers, found a lack of sufficient depth of instruction and reported that "there are no requirements for MET institutions to include cybersecurity awareness or cyber hygiene practice in the curricula," (p. 49). They did note, however, that this may be attributable to the slow process of changes in international maritime regulations that inhibit agility in shifting MET curricula and courses.

This review of existing maritime cybersecurity education-related literature leads us to conclude that, in the current environment, MET institutions face challenges in rapidly addressing the pressing cybersecurity education needs. Thus, there likely is value in bringing cybersecurity expertise to the maritime community from non-MET higher education institutions to complement efforts being made within MET institutions.

3. CYBERSECURITY EDUCATION COMMONS

We believe that students at many cybersecurity programs outside of MET institutions are likely to already be well-positioned to engage with maritime cybersecurity. This conjecture is based on the close ties that can be seen between published maritime industry cybersecurity guidance and published non-maritime specific guidance, on industry-neutral cybersecurity vocabulary promoted by maritime organizations, and on several informal conversations with current maritime cybersecurity personnel.

In an apparent effort to adopt useful and established cybersecurity tools, as well as a common cybersecurity language, the maritime community has embraced existing non-maritime specific cybersecurity efforts like the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018). In their published cybersecurity guidance, both the IAPH (2020) and the IMO (2021a) directly reference the five concurrent and continuous functions of the NIST framework core (Figure 4), while the ICS (2021) explicitly acknowledges taking the five functions into account during the development of their guidelines. This is a framework with which cybersecurity students from most programs are almost certainly already familiar.

Using risk-based activities to complement compliance actions when securing network and device hardware/software has become more commonplace (Lin & Saebeler, 2019) and risk-based approaches are likely to be less industry specific than compliance-based ones. The NCAE-C program document (NSA, 2019) that lists the details of CAE cyber defense (CAE-CD) knowledge units (KU) reflects the non-industry specific teaching of risk-related cybersecurity.

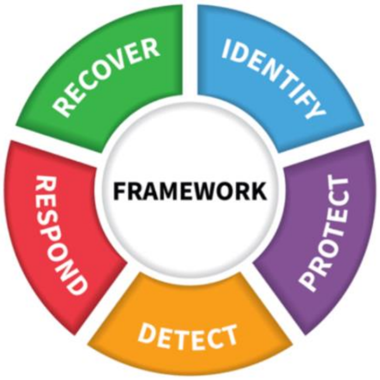


Figure 4 – framework core five concurrent and continuous functions (NIST, 2022)

The Cybersecurity Foundations (CSF) KU, one of three mandatory foundational KUs that must be satisfied be every CAE-CD designated institution, explicitly requires risk management, basic risk assessment, and residual risk be covered. The non-technical core KU, Security Risk Analysis (SRA), which is likely covered by most CAE-CD schools, plainly states an intent "to provide students with sufficient understanding of risk assessment models, methodologies and processes such that they can perform a risk assessment of a particular system and recommend mitigations to identified risks," (NSA, 2019, p. 29). Fundamental knowledge of risk-based approaches to cybersecurity is usable across all sectors.

A review of the enumerated key vocabulary in the published ICS and IAPH cybersecurity guidance reveals no maritime-unique terms. Of the 96 terms listed and defined – 40 in the ICS guidelines glossary (2021) and 56 in the IAPH white paper (2020) – 84 are unique and 12 overlap (see Appendix B). Current post-secondary cybersecurity students in NCAE-C, or similar quality, programs should find most, if not all, of these 84 terms to be familiar. Most of them are explicitly mentioned in the 2020 CAE-CD KU document (NSA, 2019).

Over the past several months, we have engaged in informal discussions regarding maritime cybersecurity with several current maritime professionals. They have varying degrees of awareness of and responsibility for cybersecurity within their respective organizations and hold jobs like Coast Guard cybersecurity specialist and port security analyst. These professionals confirmed the centrality of the NIST framework for maritime operations and supply chain partners, as well as other NIST special publications (SP) like SP 800-171r2 (Ross et al., 2020) for protecting unclassified information and SP 800-53r5 (Joint Task Force, 2020) which outlines security and privacy controls. Each also indicated a belief that students with a broad understanding of cybersecurity topics could readily contribute to the maritime community without industry-specific knowledge. Of course, having maritime-specific knowledge was better than not having it, but lack of industry-specific information would not preclude them from contributing and such knowledge likely could be readily picked up on the job.

4. READYING NON-MET CYBERSECURITY STUDENTS FOR MARITIME

An opportunity appears to exist for cybersecurity programs to further develop students by readying them for industry-specific specialization, like maritime, where intersecting interests and potential value are present. We take as a premise that the educational objective for industry sector specialization is to pull forward knowledge that is typically received via on-the-job training (OJT). If provided in the classroom under controlled conditions, the possibility exists for accelerated learning and for cyber defenders to show up better prepared on day one of employment.

Analyzing the results of our review of maritime cybersecurity education, we make six recommendations in support of maritime cybersecurity specialization education. These recommendations are made envisioning a relatively short two - four course maritime specialty, focus, concentration, or track within an existing cybersecurity program.

First, a generalized introduction to the maritime industry would provide students interested in maritime with an orientation to the sector that would later support better contextual learning.

Recommended educational content includes broadly covering topics like ships and ship operations, ports and port operations, life at sea, crew roles, an overview of digital systems employed for maritime enterprise mission achievement, etc. Furthermore, the maritime sector has a unique threat profile; understanding the types of actors interested in cyberattacks on the maritime sector, including the interaction with forms of piracy, are important in understanding the overall threat (Jones et al., 2016). This introduction will be useful for developing and understanding a maritime mental model or framework. Establishing this mental model/ framework would help prepare students to defend a maritime enterprise more successfully.

Second, given the regulated nature of the maritime industry, introducing students to the rules of the game is important. Existing regulations are currently being updated to include cybersecurity by controlling authorities like the U.S. Coast Guard, the IMO, flag states of convenience for vessel registration, etc. Gaining a basic understanding of relevant regulations and their scope will better prepare students for the compliance side of maritime cybersecurity.

Third, knowledge, skills, and abilities (KSAs) are mapped to cybersecurity work roles in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (National Initiative for Cybersecurity Careers and Studies, 2022; Peterson et al., 2020). This concept can be extended to the roles in a maritime enterprise. It is widely acknowledged that every enterprise employee is responsible for cybersecurity. Therefore, it is important for students to understand cybersecurity KSAs for employee types within an enterprise. This information will help students understand how to set up training programs to enhance enterprise cybersecurity.

Fourth, there are enterprise behaviors unique to the maritime industry the awareness of which will be valuable for students. For example, personnel on board a ship are typically temporary contract workers employed for six or nine months. Therefore, ships experience a higher personnel turnover rate than most land-based enterprises and this, in turn, creates additional cyber risk. Another example is that ship IT infrastructure is serviced in remote ports of the world by third-party contracted service technicians. These technicians have direct access to ship IT infrastructure and present a potential cyber risk.

Fifth, collaborations between MET and non-MET institutions can help complement the strengths of each. METs often have specialized equipment, from simulation rooms to a variety of training watercraft, that could be used by non-MET students and faculty to gain hands-on experience. Non-MET institutions can bring their cybersecurity expertise and facilities to bear by offering advanced training opportunities and a wider geographic footprint of opportunities. Faculty from MET and non-MET institutions could exchange ideas and best practices developed in different contexts and work together on enhancing their respective curricula.

Sixth, the creation of new, tangible classroom teaching aids will provide students with an active versus passive lecture-based learning experience. The creation of a maritime mental model/framework, the expected result of the first recommendation, helps place follow-on maritime cybersecurity instruction within a useful context. Interactive aids that bring the enterprise into the classroom, likely the best alternative we have to actual work experience, will help cybersecurity students visualize the relevant, associated attack surfaces. Being able to view an image of the digital enterprise being defended and its operating environment versus imagining an abstract, nondescript enterprise will likely accelerate student understanding.

Crafting a maritime focus within an existing cybersecurity program using the guidance offered by these six recommendations should provide a solid head start to any student interested in the maritime industry. In the next section, we elaborate on the sixth recommendation and its potential for industry-focused cybersecurity.

5. INTERACTIVE AIDS FOR FOCUSED CYBERSECURITY

Many cybersecurity students are taught the theory of NIST's cybersecurity framework (Figure 4) and likely apply the theory to one or more case studies. However, the industry in the case study is unlikely deliberately chosen and the assignment is likely primarily a mental exercise focused primarily on the framework rather than balanced with gaining understanding of and insight into an industry.

The type of teaching aid we envision with our fifth recommendation in the previous section is one that allows students to *see* the environment they are defending. Our guiding precept – coined Greer's Rule of Thumb – is that: *it is impossible* *to defend what cannot be visualized and described*.

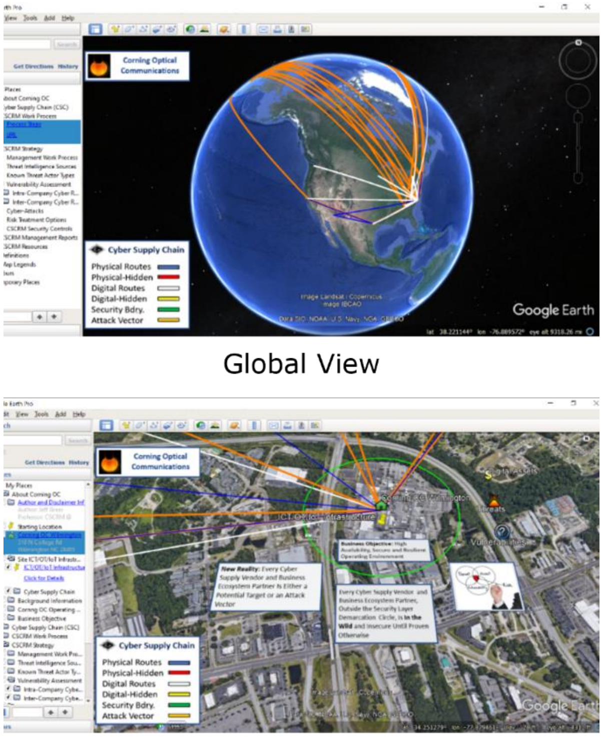
This requirement seems best met by the development of an interactive environment like the integrated virtual learning environment for cybersecurity education (IVLE4C, Greer et al., 2022). Whereas traditional cyber ranges are network centric, IVLE4C presents a holistic view of all elements in an enterprise's attack surface. The initial version of IVLE4C was a low-cost option developed using Microsoft Office and Google Earth Pro (Figure 5), but it already provides something with which students will be able to clearly visualize the enterprise they are defending, and it is easily adaptable to visualizing maritime enterprises like ports and terminals.

Students need to understand how the particular enterprise type and particular enterprise behaviors impact the corresponding attack surface structure. Each attack surface element has inherent vulnerabilities that can be exploited if left untreated. The objective of risk management is to change the attack surface elements into trust boundaries at a level sufficient to meet enterprise cybersecurity requirements. It is also useful for students and cybersecurity professionals who will have varying levels of information when working to defend a modern digital enterprise.

Any given maritime enterprise, a complex system of systems, needs to be analyzed in terms of assets of value, threats, and known vulnerabilities. These are the three elements required to form a picture of risk. Students need to be taught how to enumerate risks in a register. Once recorded in a register, students need to be taught how to assess them using a heat matrix, ranking identified risks from high to low. An interactive aid, like IVLE4C, will help cybersecurity students more quickly learn this process and appreciate how theoretical frameworks directly relate to the physical operating environment.

A risk register serves as an artifact for designing a risk treatment plan. Students need to be taught how to utilize the standard ISO 31000 Risk Management Framework options to treat each recorded risk. Once a risk treatment plan is complete, students need to be taught how to implement it using sound project management practices. This can be accomplished by teaching a student how to develop a plan of action and milestones (POAM). Conducting all these steps while referencing and interacting with a visualization of the defended enterprise should accelerate students' understanding of the industry of focus.

Modeling an enterprise is not a new idea in cybersecurity education. It is also not new in maritime where simulators are commonly used for teaching navigation. What is underdeveloped is the application of modeling in developing enterprise cybersecurity solutions in the maritime industry and other critical infrastructure sectors. Creating a virtual environment where students can work at the enterprise system of systems level across multiple critical infrastructure sectors will facilitate advanced cognitive and cybersecurity skills development that are needed by future cybersecurity leaders.



Global View

Enterprise Operating Site

Figure 5 – IVLE4C v1 global view and enterprise operating site view

6. CONCLUSIONS

In this paper, we examined the current state of cybersecurity and cybersecurity education within the maritime community as reflected in the academic and professional literature. We found that the industry's cybersecurity posture lags other sectors and that a gap appears to exist in cybersecurity education within current MET curricula. Given the pressing challenge of the cybersecurity workforce shortage, it seems plausible that the maritime industry as well as governmental agencies in the maritime sector would benefit from the cybersecurity education produced by non-MET institutions as well.

In answer to the two questions posed in the introduction, we suggest that students in non-MET cybersecurity programs are well-positioned with their existing knowledge to contribute to the maritime community's cybersecurity efforts. By incorporating maritime-specific knowledge into their education, these students could readily contribute to the maritime sector immediately after graduation. We further suggest six ways to incorporate a maritime focus into an existing cybersecurity curriculum and then elaborate on the suggestion related to interactive teaching aids designed to bring the enterprise into the classroom.

7. REFERENCES

Accreditation Board for Engineering and Technology. (2022a, July). ABET approves accreditation criteria for undergraduate cybersecurity programs. https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/

Accreditation Board for Engineering and Technology. (2022b, July). Accredited Programs. https://amspub.abet.org/aps/category-search?disciplines=91&disciplines=94

Ahvenjärvi, S., Czarnowski, I., & Mogensen. J. (2019, August). Addressing Cyber Security in Maritime Education and Training (CYMET). FY2018 IAMU Research Project. http://archive.iamu-edu.org/download/final-report-of-research-project-fy2018/

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. Network, 2(1), 123-138. https://www.mdpi.com/2673-8732/2/1/9/pdf

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554. https://cyberonboard.com/wp-content/uploads/Critical-Infrastructures-Cybersecurity-and-the-Maritime-Sector.pdf

Alop, A. (2019, April). The challenges of the digital technology era for maritime education and training. In 2019 European Navigation Conference (ENC) (pp. 1-5). IEEE. https://www.researchgate.net/publication/333152469_The_Challenges_of_the_Digital_Technology_Era_for_Maritime_Education_and_Training

Bacasdoon, J. (2021). A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches. https://commons.wmu.se/all_dissertations/1680/

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. Intellectual Property & Technology Law Journal, 27(1), 16. https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cybersecurity-10-2014.pdf

Center of Academic Excellence in Cybersecurity Community. (2022a, July). CAE institution map. https://www.caecommunity.org/cae-map

Center of Academic Excellence in Cybersecurity Community. (2022b, July). What is a CAE in Cybersecurity? https://www.caecommunity.org/about-us/what-cae-cybersecurity

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review. In Proceedings of the international association of Maritime Universities (IAMU) Conference. http://researchonline.ljmu.ac.uk/id/eprint/11929/1/IAMU%202019%20Park%20et%20al.pdf

Cyber Seek. (2022, July). Cybersecurity Supply/Demand Heat Map. https://www.cyberseek.org/heatmap.html

de Bont, J. (Director). (1997). Speed 2: Cruise Control [Film]. Blue Tulip Productions; 20th Century Fox. https://www.imdb.com/title/tt0120179/

de la Peña Zarzuelo, I., Soeane, M. J. F., & Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. Journal of Industrial Information Integration, 20, 100173. https://www.Sciencedirect.com/science/article/pii/S2452414X20300480

Demchak, C. and Thomas, M. (2021, October 15) Can't Sail Away From Cyber Attacks: 'Sea-Hacking' From Land. War on the Rocks. https://warontherocks.com/2021/10/cant-sail-away-from-cyber-attacks-sea-hacking-from-land/

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015, July). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE. http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf

Gliha, D. (2017). Maritime Cyber Crime-21st Century Piracy. Annals of the Faculty of Law of the University of Zenica, 20, 228-238. https://heinonline.org/HOL/Page?handle=hein.journals/zenici20&div=15&g_sent=1&casa_token=&collection=journals

Greer, J., Stoker, G., & Clark, U., (2022). Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C). Cybersecurity Pedagogy and Practice Journal1(1) pp 54-65. http://cppj.info/2022-1/n1/CPPJv1n1p54.pdf

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In Developments in Maritime Technology and Engineering (pp. 49-61). CRC Press. https://www.researchgate.net/profile/Dan-Heering/publication/353924133_Shortcomings_in_cybersecurity_education_for_seafarers/links/611a34d00c2bfa282a49e898/Shortcomings-in-cybersecurity-education-for-seafarers.pdf

International Association of Ports and Harbors. (2020, June). Port Community Cyber Security. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

International Chamber of Shipping. (2021). The Guidelines on Cyber Security Onboard Ships v4. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

International Maritime Organization. (2017, June 16). Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

International Maritime Organization. (2021a, June 14). Guidelines on Maritime Cyber Risk Management. MSC-FAL. 1/Circ. 3/Rev. 1. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

International Maritime Organization. (2021b). Introduction to IMO. https://www.imo.org/en/About/Pages/Default.aspx

Joint Task Force, National Institute of Standards and Technology. (2020, September). Security and privacy controls for information systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Joint Task Force on Cybersecurity Education. (2022, July). ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. https://cybered.hosting.acm.org/wp/

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. IET Engineering & Technology Reference.

Lin, W. & Saebeler, D. (2019). Risk-based v. compliance-based utility cybersecurity a false dichotomy. Energy Law Journal, 40(2), 243-282. https://www.eba-net.org/assets/1/6/8._[Lin_and_Saebeler][Final][243-282].pdf

Loomis, W., Singh V. V., Kessler, G., and Bellekens, X. (2021, October) Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. Atlantic Council Scowcroft Center for Strategy and Security.

National Academy of Public Administration. (2021, November). Organizational Assessment of the U.S. Merchant Marine Academy: A Path Forward. https://s3.us-west-2.amazonaws.com/napa-2021/NAPA-Panel-Report-FINAL.pdf

National Initiative for Cybersecurity Careers and Studies. (2022, July). Workforce Framework for Cybersecurity (NICE Framework). https://niccs.cisa.gov/workforce-development/nice-framework

National Institute of Standards and Technology. (2022). Cybersecurity framework. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2018, April 16). Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Security Agency. (2019, June 7). 2020 CAE cyber defense (CAE-CD) knowledge units. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Noel, A., Shreyanka, K., Gowtham, K., & Satya, K. (2019, November). Autonomous ship navigation methods: a review. Proceedings of the International Conference on Marine Engineering and Technology (ICMET) Oman. https://www.researchgate.net/profile/Shameem-Bm/publication/338338942_Autonomous_Ship_Navigation_Methods_A_Review/links/5e4aa5cd92851c7f7f425403/Autonomous-Ship-Navigation-Methods-A-Review.pdf

O'Brien, R. C. (2021, January 5). Statement from National Security Advisor Robert C. O'Brien Regarding the National Maritime Cybersecurity Plan. https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-regarding-national-maritime-cybersecurity-plan/

Peterson, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020, November). NIST SP 800-181r1. Workforce Framework for Cybersecurity (NICE Framework). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Pyykkö, H., Kuusijärvi, J., Silverajan, B., & Hinkka, V. (2020). The Cyber Threat Preparedness in the Maritime Logistics Industry. Proceedings of 8th Transport Research Arena, 27-30. https://www.corealis.eu/wp-content/uploads/2020/05/TRA2020_Cybersecurity_article_Pyykko_et_al..pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020, February). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Satira, Brian. (2021, May 12). Navigating the Waters of Maritime Cybersecurity. Helpnet Security. https://www.helpnetsecurity.com/2021/05/12/maritime-cybersecurity/

Schwab, K. (2017). The fourth industrial revolution. Currency. https://jmss.vic.edu.au/wp-content/uploads/2021/06/The_Fourth_Industrial_Revolution.pdf

United Nations Conference on Trade and Development. (2021). Review of maritime transport. https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport

U.S. Coast Guard Academy. (2022, July). Cyber systems accreditation. https://www.uscga.edu/cyber-systems/

U.S. Government Accountability Office. (2014). Maritime critical infrastructure protection: DHS needs to better address port cybersecurity. https://www.gao.gov/assets/gao-14-459.pdf

U.S. Naval Academy. (2020, November 6). USNA cyber operations program granted NSA designation. https://www.usna.edu/NewsCenter/2020/11/USNA_CYBER_OPERATIONS_PROGRAM_GRANTED_NSA_DESIGNATION.php

White House. (2020, December). National Maritime Cybersecurity Plan to the National Strategy for Maritime Security. https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

Editor's Note:

This paper was selected for inclusion in the journal as an ISCAP 2022 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.

Appendix A – Acronyms of Common Maritime Systems

AIS – automatic identification system
ECDIS – electronic chart display and information system
EPIRB – emergency position-indicating radio beacon
GMDSS – global maritime distress and safety system
GNSS – global navigation satellite systems
GPS – global positioning system
SATCOM – satellite communications
VHF – very high frequency

Appendix B – Cybersecurity Key Terms

This appendix lists the 84 unique terms pulled from the combined list of 96 terms (12 overlapping) from the 40 terms of the ICS' Guidelines on Cyber Security Onboard Ships v4 (2021) and the 56 terms of the IAPH's Port Community Cyber Security (2020).

Access control	Data breach	Operational technology (OT)
Adware	Defence in breadth	Patches
Advanced Persistent Threat (APT)	Defence in depth	Phishing
Antivirus (AV)	Digitisation	Principle of least privilege
Authentication	Digitalisation	Ransomware
Authorization	Encryption	Recovery
Accounting	Event and Incident response	Removable media
Availability	Executable software	Risk assessment
Back door	Firewall	Risk management
Backup	Firmware	Sandbox
Business Impact Analysis	Flaw	Service provider
Bring your own device (BYOD)	Incident	Social engineering
Chain of custody	Industrial Internet of Things (IIoT)	Software whitelisting
Computer Emergency Response Team (CERT)	Information Technology (IT)	Spam
Computer Security Incident	Information sharing and communications	Spear phishing
Confidentiality	Insider threat	Spoofing
Contingency plan	Integrity	Spyware
Cookie	Intrusion Detection System (IDS)	Supply chain risk
Cyber attack	Intrusion Prevention System (IPS)	Threat
Cyber ecosystem	Information Sharing and Analysis Center (ISAC)	Threat and vuln management
Cyber governance	Least privilege	Threat assessment
Cyber incident	Local Area Network (LAN)	Threat profile
Cyber risk management	Malware	Typo squatting
Cyber security	Maturity	Virtual Local Area Network (VLAN)
Cyber security plan	Manufacturer	Virtual Private Network (VPN)
Cyber security policy	Monitoring	Virus
Cyber security program	Multifactor Authentication (MFA)	Vishing
Cyber system	Operational resilience	Wi-Fi

Command and Control – Revisiting EATPUT as an IS Model for Understanding SIEM Complexity

Anthony Serapiglia
Anthony.Serapiglia@stvincent.edu
CIS Department
Saint Vincent College
Latrobe, PA 15650

Abstract

Automation of network security systems has led to ever increasing complexity and opaqueness. Ceding command and control actions to systems that are fully or even partially unknown to administrators can lead to possibly catastrophic results. Theoretical abstract models can aid in gaining visibility and insight into the construction and operations of these systems. This paper will utilize the early command and control information system model EATPUT to allow a better understanding of the stages and operation of a modern Security Incident Event Management (SIEM) system.

Keywords: EATPUT, Information Systems, SIEM, Cybersecurity Models

1. INTRODUCTION

The "4 V's" of Big Data – Volume, Velocity, Variety, and Veracity (Cerniauskas, 2022) also affect the practice of cybersecurity. The past several generations of computing have all seen paradigm shifts in these areas that have demanded change in how hardware, software, process, and people deal with the deluge. Much of this change has been to increase automation and look to solutions of scale that can respond to events in real-time (Andrade & Tores, 2018). This has led to ever increasing complexity and "black box" solutions that do not allow for much, if any, visibility of the system to managers or end users. While this may be convenient in terms of end users who just want working systems and protection and are little concerned with what is under the hood, for administrators, system designers, and security experts the lack of visibility is a vulnerability itself.

Projecting to abstract models is an accepted andtime-honoredd method of systems analysis and understanding of complex systems (Dorodchi et al., 2021; Thomas et al., 2021). As cybersecurity systems have evolved to adapt to the increasing demands of the current environment, what were once stand alone and isolated components have developed into integrated solutions with a much broader scope of engagement. Security Incident and Event Management (SIEM) systems are the current standard for a robust and comprehensive security solution. Combining elements of network and end host security solutions, the SIEM can extend tentacles into every element of a system to include cloud, data center, workstation, and mobile systems and devices. The SIEM is the essential "Command and Control" nexus for administrators and cybersecurity operations of today. Many current SIEM solutions include aspects of artificial intelligence and machine learning to automate response to detected suspicious activity. If this essential activity of command and control is being allocated to automated systems, those systems should be completely understood and known to those who are administering them. Unfortunately, with the increased complexity of these systems, this is often neglected out of difficulty or ignorance.

The purpose of this paper is to highlight how an abstract information system model can be used to project the components and actions of a modern SIEM to allow for insight and visibility into the system so that the "system" can be "known" and more effectively configured and optimized, especially for student unfamiliar with the system.

An early model of a command-and-control Information System, EATPUT, will be used. This model was developed in the early 1960s as part of foundational efforts in defining Decision Support Systems (DSS), Advanced Data Information and Knowledge (ADIK) systems, and the field of Information Science (NATO Advanced Study Institute in Information Science, 1974). The acronym EATPUT represents an information system defined by the focus areas of Event World, Acquisition, Transmission, Processing, Utilization, and Transfer. Having origination ties to the development of military command and control systems, EATPUT is an ideal candidate model to allow insight into the complex SIEM systems of today.

2. AN EVOLUTION OF VISIBILITY

Network Security provides an area for a stark example of the progress in the evolution of Cybersecurity as technological advances in both hardware and software have allowed more automated solutions. In *The Cuckoo's Egg* (1989) Stoll provides a view into how a network intrusion could be detected and traced in a time before the commercial Internet of today. In it, Stoll describes a process of data capture in which he manually connected teletype machines and printers to modem lines in an effort to capture traffic generated by an intruder to the system. By the end of the 1990's, Intrusion Detection Systems (IDS) were common in most consumer grade router equipment. But just like the efforts of Stoll in the 1980s, all of those logs were meaningless unless someone laid eyes on them and took action on what they saw. With an ever-increasing volume of data leading to ever increasing volumes of logs, the workload quickly overcame the ability of humans to lay eyes on everything.

IDS/IPS

Enter the Intrusion Detection System (IDS). As detection systems continued to develop and gain sophistication, they became very proficient at being able to identify threats on multiple platforms from in the network stack to an individual host. Unfortunately, seeing an attack as it occurs is one thing; stopping it is another. Preventing downtime is one of the highest priorities of any administrator (See the "A" in CIA…), in the end, an IDS on its own often does little to meet this demand. As features continued to be added to these systems, however, their ability to react also continued to grow. Early advances led to the ability to simply reset a connection or blacklist an originating IP Address. While effective in a short window of an attack in progress, these are inherently reactive responses and are easily worked around by a persistent or intelligent threat actor. However, anything more sophisticated requires more logic and also more data, requiring deeper packet inspection which in turn requires more horsepower from the networking equipment. Access Control decisions made by firewall/router devices began to be informed by the greater insight provided by the deeper inspection of packets on the IDS side. Equipment manufacturers eager to move on from a product line that was seen as insufficient were quick to brand a new product line – the IPS (Gartner, 2016). An Intrusion Prevention System (IPS) is an in-line networking product that focuses on identifying and blocking malicious network activity in real time (Fuchsberger, 2005). With the pace of development spurred by the appearance of more cyber threats in the early 2000's, nearly all modern router devices began to contain an integrated firewall feature expanded to include some IPS components in the system by 2005, according to the Gartner Group, as they termed the solution the Next Generation Firewall (NGFW) (Hils, 2015).

Much has changed in the threat landscape in the past 20 years. To borrow a phrase, the landscape is 'everything, everywhere, all at once.' While "visibility" into network traffic has always been a challenge, even dating back to the era of Stoll and his typewriters hooked to modems, the challenge facing administrators of this current system evolution is the need to have visibility, really, for everything – everywhere – and all at once. Distributed systems have placed devices, processes, storage, and vulnerabilities across the globe and into the cloud. Tracking traffic and threats must happen in all of these places. The "in-line network appliance" can only see so much. To gain full insight and vision into a modern system, agents, clients, daemons, widgets must be integrated into end-user devices and applications at all levels.

How to be everywhere?

Security Incident and Event Management (SIEM) systems are a solution that helps organizations recognize potential security threats and vulnerabilities before they have a chance to disrupt business operations. It surfaces user behavior anomalies and uses Artificial Intelligence to automate many of the manual processes associated with threat detection and incident response and has become a staple in modern-day security operation centers (SOCs) for security and compliance management use cases (IBM, 2022). SIEMs have matured to become more than just log management tools. A modern SIEM offers advanced user and entity behavior analytics (UEBA) leveraging the power of Artificial Intelligence and machine learning. A SIEM is a highly efficient data orchestration system for managing ever-evolving threats as well as regulatory compliance and reporting that can function across locations, networks, and device infrastructures. A SIEM system gathers data from many sources, correlating all the available information available. This lets it not only detect active threats but find hidden weaknesses and threats. Its inputs include system and application logs as well as live IDS and IPS data.

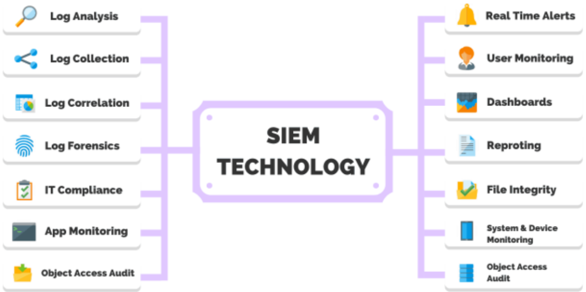


Figure 1 – SIEM Model (Firch, 2021).

The core capabilities of a SIEM include: log event collection and organization including contextual data sources; the ability to analyze log events and other data across disparate sources; operational capabilities such as incident response, dashboards, and reporting; support for threat detection; and compliance commitments including security incident reporting for management.

Implementing SIEMs at the highest level has allowed many security controls to be automated within organizations. This automation has allowed faster reaction times to threat actors achieving more efficiency in Information Security management overall. The inclusion of automation tools has reduced the complexity of command chains that are often involved in the response process (Montesino, Fenz, & Baluja, 2012).

3. EATPUT

Dr. Anthony Debons was an experimental psychologist and early pioneer in Information Science. Debons worked closely with the Army Air Corps and US Air Force in the years after World War II developing command and control systems. These were heady days of advancements in Information Systems, Decision Support Systems, and ADIK (Advanced Data Information Knowledge) systems. While these specific labels may have gone out of favor, their core simplicity in structure and framework is worth revisiting as models for modern "complex" systems.

Beginning in 1960, Debons led a project to establish a conceptual framework for the design of an information system to support command and control for the Strategic Air Command. This project was a contemporary of the time of the group led by J.C.R. Licklider at DARPA, with Debons and Licklider both having backgrounds in psychology and wide interdisciplinary views of information systems. According to Debons, they conferred on a number of occasions at the time, including consultations on funding devoted to projects to develop better software and to train more computer programs that would benefit both of them (Asprey, 1999). These efforts in developing command and control systems for the military had great influence on the development of early management information systems and decision support systems leading to Management Information Systems of today (Asprey, 1999).

Command and Control

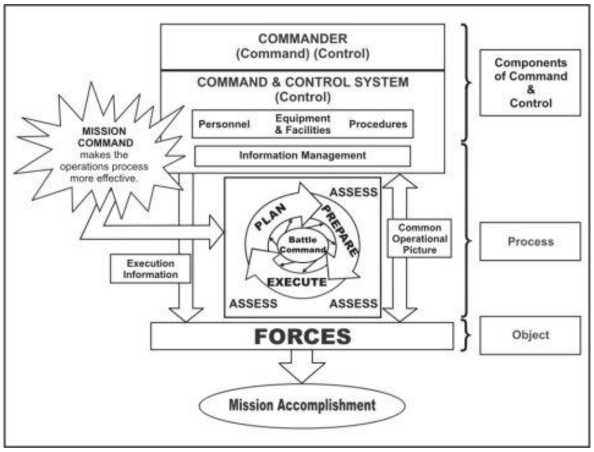


Figure 2. Command and Control (US Department of the Army, 2003).

It was during his work with the Strategic Air Command that Debons and his team of junior officers developed an intellectual framework for the structure of a hypothetical information system. There was agreement that the computerization of a command-and-control system might be considered as an information system (Aspry, 1999). As such "…the science and technology related to the command-and-control functions is primarily directed in achieving one objective, namely, aiding man to make the best use of the data about his environment for decision making (Debons, 1971).

"Command and control is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of a mission. Commanders perform command and control functions through a command-and-control system" (U.S. Department of the Army, 2003).

Three characteristics of effective command and control are: ability to identify and react to changes in the situation; ability to provide a continuous, interactive process of reciprocal influence among the commander, staff, and available forces; and ability to reduce chaos and lessen uncertainty.

The Model

The generalized Information System model that Debons arrived at is known as EATPUT. Consisting of six basic components, the first letters of which produce the acronym. The six components of EATPUT are:

Event World – The occurrences that are relevant to the objective and functioning of the information system. It includes the classifying and categorizing of events and the representation of them in symbolic form.

Acquisition – The initial physical component of the system, used to capture matter and energy describing an event from the external environment (data).

Transmission – The actual movement of signals (data) within and between components of the system.

Processing – The ordering, storage, and retrieval of data for the ultimate purpose of applying it to problem solving, decision making, or general development (knowledge formulation).

Utilization – The component that represents the evaluative, interpretive requirement of information systems

Transfer – the action component of the system; the implementation of the decider function through the system's transfer medium. The Transfer function in this model can be seen as communication or information transfer (Debons, Horne, Cronenweth 1988).

As a model, there are obvious similarities to computing models that were contemporary of the time, such as a simplified Von Neumann model of Input – Processing – Storage – Output construction. However, Debons refused to be constrained by restricting his model to computer constructs. S.J. Keyser, a former Rhodes scholar and specialist in linguistics was part of Debons's team in the early 1960's with the US Air Force. It was Keyser who introduced the idea to Debons that human beings existed as information systems. An organism, such as a human, had all the necessary functional elements to form an information system. The integration of human factors into the theoretical work of constructing an automated information system was novel at the time. According to an interview with Debons in 1988, "Command and Control had not achieved a synthesizing construct. The major concept of command and control rested on computer development to support machine data processing – given presence through the electronic display technology. The basic fallacy of this construct was its lack of attention to the role of sensors, teletransmission, and other technological constituents that assume presence to augment human organismic capabilities" (Aspray, 1999).

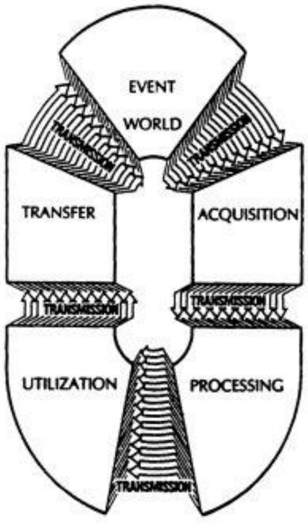


Figure 1 EATPUT as a cyclical model (Debons, Horne, Cronenweth 1988).

4. SIEM – C&C – EATPUT

A SIEM system can be one of the most complex components of a layered cybersecurity solution. Even in the most basic of implementations, a SIEM aggregates log data, security alerts, and event logs from multiple different devices from multiple different manufacturers, utilizing multiple different protocols into a centralized platform to provide real-time analysis for security monitoring (Gast, 2021). Next-Gen SIEMS are already in place that are leveraging AI techniques with User Entity Behavior Analytics (UEBA) to automate sophisticated responses to detected deviations from standard baseline operations (Cooper, 2022).

Given this level of complexity, it is no wonder that many students view the SIEM as a black box without actually understanding the inner components. Yet it is that complexity that can be utilized in cybersecurity education as an evaluation tool in gauging the student's depth of understanding of systems, their components, interactions, and complexity. "SIEM coverage is needed because cybersecurity education is often perceived by students to be fragmented and disjointed as there are many seemingly overlapping, conflicting and diverging topics. SIEM systems demonstrate an overview and dashboard displaying the current cybersecurity posture providing a framework to students allowing them to understand the relationship among the many components and topics within cybersecurity" (MacDonald, 2020.)

One of the driving factors of Debons' work of the 1960s was Electronic Systems Command. As part of the Strategic Air Command, this early work on Information Systems led to command-and-control systems that helped to prevent a nuclear holocaust during the Cold War. When comparing the stakes, securing a corporate system is not quite on the same level as preserving humanity. However, the comparison holds in looking at the generalities of the complex event environment, range of possible input data, need of data processing/analytics, tuning and validation of possible responses, and the transfer of a probable solution out of the system and into the hands of an entity that can take action. Projecting a SIEM to EATPUT is possible, and natural.

SIEM to EATPUT

Mapping the concept of a modern SIEM to a foundational model of an information system such as EATPUT is a valuable exercise that can help identify gaps in a student's understanding of the complex system. The six components of the EATPUT model easily map intuitively to the components and stages of operation of a SIEM. This projection can be utilized as an instrument to aid in a systems analysis assignment.

To begin, it is important to recognize from the outset that a SIEM is an information system whose purpose is to aid decision making in responding to security events. Stating this from the start establishes the premise and can act as a type of hypothesis statement that is then proven through the subsequent mapping of components and actions to the stages of EATPUT. The event world of a Cybersecurity landscape is endless. The system is always bigger than one thinks it is. Yes, it runs from the known knowns to the unknown unknowns. A SIEM will exist within a network. It will be up to the administrator to establish the scope of the environment that the SIEM will be monitoring. Understanding the "Event World" of the specific environment will inform the extent to which the SIEM should extend. This is not about identifying all potential threat actors or even threats. It is about identifying the assets within your network and work environment that will need to be protected. You cannot protect it properly if you do not know it exists.

One of the key differences between the modern SIEM and traditional IDS/IPS is positioning. IDS/IPS are primarily found in line with the networking stack. More software solutions have been implemented as a part of all-in-one protection suites, but the primary positioning is away from the user and at the border of the network. As an administrative tool, pieces of the SIEM can exist anywhere. The more devices and locations agents and probes can exist, the more robust the SIEM can be. The more data a SEIM collects, the more insight it can provide. The "Acquisition" stage of EATPUT is the piece of the model that focuses on the need to bring representations of activity in the Event World into the system. SIEMs have been able to flourish in an environment of greater interoperability. For generations, many device manufacturers were very proprietary with their products. Management tools and dashboards had to be from within the family of products. Open-source platforms and standard protocols have led to a greater ability to reach to many different areas within your environment. Many open source SIEM products exist that will enable the collection of event logs and data from Microsoft, HP, Dell, and even Apple products.

The word system has a natural inference that multiple components exist. If there are multiple components, then it is necessary that those components must be connected. If lines of communication have not been intentionally established, then it cannot be assumed that they exist. There are a number of communication and networking protocols to allow for data transfer today. From protocols such as SMB, SNMP, TCP/IP, UDP – all can facilitate background data transfer locally or across distributed systems.

Ethernet, Wi-Fi, 5G Wireless data, Bluetooth – all can serve as a channel of communication between devices and collection points. The ability to move data has never been more robust in capacity, speed, or flexibility. The key in the "Transmission" phase of EATPUT theoretically and a SIEM practically is that connectivity between components is addressed. Even with all of the options available, too often this stage, or component, is just assumed to be in place. Often it is too late when it is discovered that it has been ignored or put on the back burner and forgotten. This can lead to costly overruns in time and budget while a possible workaround is devised, if one is even possible.

The "Processing" stage in both EATPUT and within a SIEM is very direct. It is the logic component of the SIEM where data is massaged, sorted, shifted, and otherwise worked with. The intelligence of the application is located here. This is the collected and customized set of rules that have been created to interpret the data. Concrete rules, adaptive logic, heuristics, and now some form of Artificial Intelligence can all be combined to identify threats and possible reactions. It is important to note, the result of processing is a possible solution to the problem or issue at hand. The result of processing is not the end – it is a stage. More needs to be done with the possible solution before it can be moved outside of the information system/SIEM and applied in the Event World.

The "Utilization" stage of EATPUT can be looked at in two different ways. From the perspective of working with the possible solution – this is a moment to remember that at this stage the possible solution is still within the system. This is a "check your work" break point opportunity to do some validation and verification of the result of processing. At this point, there is a possibility to spot-check the possible solution to ensure that it is at least in a range of feasibility. If a program is intended to be a calculator and the result of processing 2+2 is Blue – then there is no sense forwarding the possible solution outside of the system for action as it is not a feasible or viable solution to the question. In terms of the SIEM, this stage can take the form of validation of alarms and the tuning to behavioral norms for the system and environment.

From a systems builder point of view, utilization can be a reminder that every component of the system is being utilized. There has been no superfluous junk included, that the system is as compact and eloquent as possible. This is important in multiple ways. It first ensures there has been no wasted time, effort, or expenditure. It also ensures that there are no orphaned components that have been left on the side and forgotten. These are the components that may never be updated and may not even be monitored. They become a security vulnerability in their own right. In constructing a SIEM, whether open-sourced or purchased off the shelf, it can be easy to get distracted by the bells and whistles, all of the add-ons that sound great but may never be used. A SIEM system designer/implementor should build in only necessary components. Future proofing is not necessary. A good SIEM design should be flexible and the ability to bolt on extra agents or data inflows should be a painless process as needed.

A possible solution cannot be put into action until it is transferred out of the system. This is the "output" equivalency of the general computing model. Unless there is some mechanism included to display, print, or otherwise pass on a result of processing to the event world, it can never be acted upon as it would simply stay within the system and a user may never even be made aware a situation existed that needed addressing. In terms of the SIEM, this may be autonomous action through APIs and control agents, or alerting to administrators who may evaluate and determine action to maintain a layer of human decision making within the chain of command. "Transfer" does not have to be direct action, though direct action can be combined with notifications and recommendations. If a malware detection piece of a SIEM identifies that a specific workstation may have downloaded a malicious file, a robust and integrated SIEM system may quarantine the workstation by disabling the network interface card/Wi-Fi adapter on the workstation, disabling the port on a physical switch that the workstation may be attached to, begin a full anti-virus scan of the workstation, trigger an alert to a SOC/NOC/Network or Systems Administrator for follow-up and an alerting screen and messaging to the user that their workstation is temporarily out of service until cleared by the administrators.

5. CONCLUSION

In combating cybersecurity threats, network and systems administrators must employ ever more sophisticated approaches and information systems that allow for command and control over their network and computing environments. Increasingly, these systems are becoming more and more automated to allow for quicker response times to an exponential growth in data traffic, the increase in attack vectors, and the growth and variety of threat actors. An unfortunate side effect of automation is often a lack of transparency into the complex automated system (Creel, 2020). For those on the front lines using these systems every day, their intimacy allows many to eventually know every aspect. For students and beginners who have limited or no hands-on experience with these complex systems, the challenge of understanding their intricacies and parts is compounded and can be overwhelming (Sterman, 1994). By utilizing abstracted models and projecting the components and action of an automated system to it, understanding can come easier for neophytes and can lend to more insight in developing and optimizing the system for those just becoming familiar with it.

The EATPUT model was originally devised by Debons through work in developing Command and Control systems for the United States Air Force Strategic Air Command. It is a model that can be used in the current digital landscape to allow greater visibility and understanding of complex cybersecurity systems such as a SIEM. It allows for segmenting each stage of the process flow: identifying the scope of the environment; intake of data; movement of data within the system; processing to determine a possible solution; validating the system and solution; and transferring actionable intelligence back into the environment. A SIEM system is a command-and-control system. To be as effective as possible it must be understood on both a direct practical level, as well as conceptually and logically – especially as they evolve to include more Artificial Intelligence and direct-action components. Utilizing EATPUT as a conceptual model can allow for a direct systems analysis process and afford a greater understanding of the modern SIEM system.

The next generation of SIEMs have already appeared. The first SIEM systems were not originally equipped or intended to take direct action. As these features evolved, a new category of automated systems has been coined – SOAR systems: Security Orchestration, Automation and Response. This evolution is natural and expected, as will be the next. Even as these systems develop further, their essential structure will fundamentally remain the same. EATPUT will still be a model they can be abstracted to.

9. REFERENCES

Andrade, R., & Torres, J. (2018). Enhancing intelligence SOC with Big Data Tools. 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). https://doi.org/10.1109/iemcon.2018.8614779

Aspray, W. (1999). Command and control, documentation, and library science: The origins of information science at the University of Pittsburgh. IEEE Annals of the History of Computing, 21(4), 4–20. https://doi.org/10.1109/85.801528

Černiauskas, J. (n.d.). Council Post: Understanding The 4 V's Of Big Data. Forbes. Retrieved September 15, 2022, from https://www.forbes.com/sites/forbestechcouncil/2022/08/23/understanding-the-4-vs-of-big-data/?sh=7320be6d5f0a

Cooper, S. (2022, May 2). 6 best next-gen siem. Comparitech. Retrieved June 9, 2022, from https://www.comparitech.com/net-admin/best-next-gen-siem/

Creel, K. (2020). Transparency in Complex Computational Systems. Philosophy of Science, 87(4), 568-589. doi:10.1086/709729

Debons, A. (1971). Command and Control: Technology and social impact. Advances in Computers, 319–390. https://doi.org/10.1016/s0065-2458(08)60634-8

Debons, A., Horne, E., & Cronenweth, S. (1988). Information science an integrated view. G.K. Hall.

Dorodchi, M., Dehbozorgi, N., Fallahian, M., & Pouriyeh, S. (2021). Teaching Software Engineering using Abstraction through Modeling. Informatics in Education, 515–532. https://doi.org/10.15388/infedu.2021.23

Firch, J. (2021, July 23). Siem vs ids: What's the difference? PurpleSec. Retrieved July 11, 2022, from https://purplesec.us/siem-vs-ids/

Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems. Information Security Technical Report, 10(3), 134–139. https://doi.org/10.1016/j.istr.2005.08.001

Gartner_Inc. (2016, September 20). Defining intrusion detection and Prevention Systems. Retrieved July 11, 2022, from https://www.gartner.com/en/documents/3449317

Gast, K. (2022, April 29). What is Siem? and how does it work? LogRhythm. Retrieved June 11, 2022, from https://logrhythm.com/blog/what-is-siem/

Headquarters, Department of the Army. (2003). Mission Command: Command and Control of Army Forces (FM 6-0).

Hills, A. (2015, December 29). For 2016, Should We Retire the "Next Generation Firewall"? [web log]. Retrieved March 2, 2022, from https://blogs.gartner.com/adam-hils/for-2016-should-we-retire-the-term-next-generation-firewall/.

MacDonald, M., Pike, D., Pike, R. (2020). Exploring Depth in Cybersecurity Education Through the Lens of a SIEM, 2020 Proceedings of the EDSIG Conference ISSN 2473-4901 V6 n5327, November, 2020.

Montesino, R., Fenz, S., & Baluja, W. (2012). Siem-based framework for Security Controls Automation. Information Management & Computer Security, 20(4), 248–263. https://doi.org/10.1108/09685221211267639

Quigley, E. J., & Debons, A. (1999). Interrogative theory of information and knowledge. Proceedings of the 1999 ACM SIGCPR Conference on Computer Personnel Research - SIGCPR '99. https://doi.org/10.1145/299513.299602

Stoll, C. (1995). The Cuckoo's Egg: Tracking a spy through the maze of Computer Espionage. Doubleday.

NATO Advanced Study Institute in Information Science, & Debons, A. (1974). Information science: Search for identity : proceedings of the 1972 NATO Advanced Study Institute in Information Science held at Seven Springs, Champion, Pennsylvania, August 12-20, 1972. New York: M. Dekker.

Sterman, J. D. (1994). Learning in and about complex systems. System Dynamics Review, 10(2-3), 291–330. https://doi.org/10.1002/sdr.4260100214

Thomas, P. J., Patel, D., & Magana, A. J. (2021). Characterizing Student Proficiency in Software Modeling in Terms of Functions, Structures, and Behaviors. ACM Transactions on Computing Education, 21(3), 1–25. https://doi.org/10.1145/3458039

What is Security Information and Event Management (SIEM)? IBM. (n.d.). Retrieved June 6, 2022, from https://www.ibm.com/topics/si